

EXHIBIT 1

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN**

JDS TECHNOLOGIES, INC.,
a Michigan corporation,

Plaintiff,

v.

AVIGILON USA CORPORATION,
INC., a Delaware corporation, and
AVIGILON CORPORATION,
a Canadian corporation,

Defendants.

Case No. 2:15-cv-10385-AC-EAS

Hon. Avern Cohn

Magistrate Judge Elizabeth A. Stafford

**AMENDED COMPLAINT FOR PATENT
INFRINGEMENT AND JURY DEMAND**

Plaintiff, JDS Technologies, Inc., by and through its undersigned counsel, for its Complaint herein against Defendants, Avigilon USA Corporation, Inc. and Avigilon Corporation (“Avigilon”), alleges as follows:

I. THE PARTIES

1. Plaintiff JDS Technologies, Inc. (“JDS”) is a Michigan corporation having its headquarters at 59992 Ray Center Road, Ray, Michigan 48096.

2. Upon information and belief, Defendant Avigilon USA Corporation, Inc. is a Delaware corporation with its principal place of business at 1717 McKinney Avenue, Suite 1590, Dallas, Texas 75202.

3. Upon information and belief, Defendant Avigilon Corporation is a Canadian corporation with its principal place of business at 858 Beatty St, 4th Floor, Vancouver, British Columbia, V6B 1C1, Canada.

4. Defendants Avigilon USA Corporation and Avigilon Corporation shall herein be referred to collectively as Avigilon.

II. JURISDICTION

5. This is an action for patent infringement arising under the Patent Laws of the United States, Title 35, United States Code. The subject matter jurisdiction

for this Court is founded upon 28 U.S.C. § 1338 (patents) and 28 U.S.C. § 1331 (federal question).

6. Upon information and belief, Defendants are subject to this Court's jurisdiction because the Defendants regularly and continuously engage in substantial sales and other business transactions in the Eastern District of Michigan, and have sold infringing products and/or committed infringing acts in this District. Further, the Defendants maintain both sales representatives and sales partners in the State of Michigan. The United States District Court for the Eastern District of Michigan therefore has *in personam* jurisdiction over the Defendants.

7. On its website, www.avigilon.com, Avigilon maintains a "Sales Locator" tool, which identifies five sales representatives for the state of Michigan. *See* Exhibit A, Avigilon Website Capture (<http://avigilon.com/sales-locator/results/us/mi>).

8. Additionally, on its website at www.synergysystemsolutions.com, Synergy System Solutions lists Avigilon as an "Innovation Partner." *See* Exhibit B, Synergy System Solutions Website Capture (<http://www.synergysystemsolutions.com/technology-partners>). Synergy System Solutions also states on its website that it is "the area's most capable provider of technically advanced Surveillance and Access Control equipment" and maintains a

place of business at 314 N Wilson Ave, Royal Oak, Michigan 48067, which is in the Eastern District of Michigan.

9. Upon information and belief, Avigilon's video management software and/or its associated hardware is currently used in St. Joseph Mercy Oakland Hospital located in Pontiac, Michigan, which is in the Eastern District of Michigan.

10. Upon information and belief, Avigilon's video management software and/or its associated hardware is currently used in facilities of the Jackson County Intermediate School District located in Jackson, Michigan, which is in the Eastern District of Michigan. *See* Exhibit C, Jackson County Intermediate School District Video Surveillance Systems Request for Proposal dated January 20, 2014.

11. Upon information and belief, Avigilon's video management software and/or its associated hardware is also currently used throughout the campus of Kettering University in Flint, Michigan, which is in the Eastern District of Michigan. *See* Exhibit D, Kettering University Press Release dated March 20, 2013.

III. THE INFRINGED PATENTS

12. On May 10, 2005, the U.S. Patent and Trademark Office ("USPTO") duly and legally issued U.S. Patent No. 6,891,566 ("the '566 Patent"), titled "Digital Video System Using Networked Cameras." *See* Exhibit E, U.S. Patent No. 6,891,566.

13. On May 22, 2012, the U.S. Patent and Trademark Office (“USPTO”) duly and legally issued U.S. Patent No. 8,185,964 (“the ’964 Patent”), titled “Digital Video System Using Networked Cameras.” See Exhibit F, U.S. Patent No. 8,185,964.

14. JDS is the owner of all right, title, and interest in the ’566 and ’964 Patents (hereinafter the “Patents-in-Suit”), including the right to recover for infringement thereof.

15. The Patents-In-Suit are directed, *inter alia*, to software, a digital video system, and/or a method for operating a digital video system. In particular, claims are directed to software that provides for the accessing and displaying of camera images. The Patents-in-Suit include claims directed to enabling or limiting access to specific cameras.

16. JDS both designs and sells video management software and systems. The work includes developing and implementing applications, utilities, and solutions for customers in a wide variety of industries and markets. JDS markets and sells the Softsite software suite for the security industry.

IV. ACTIONS GIVING RISE TO THE COMPLAINT

17. JDS and Avigilon are competitors for the sales of video management software.

18. Avigilon is a large and sophisticated company and is aware of the intellectual property rights of others in the video management software industry. On its website at www.avigilon.com, Avigilon states that it provides “industry-leading HD network video management software and megapixel cameras [that] are reinventing surveillance.” *See* www.avigilon.com/about. Upon information and belief, Avigilon regularly conducts searches for patents related to its products. Thus, a reasonable inference is that Avigilon is aware of the Patents-in-Suit. Plaintiff asserts that this reasonable inference is true.

19. JDS prominently marks its video management software with the Patents-in-Suit. JDS has marked its video management software with U.S. Patent No. 6,891,566 since shortly after its issuance in 2005. JDS has also marked its video management software with U.S. Patent No. 8,185,964 since shortly after its issuance in 2012. Thus, Plaintiff hereby asserts that there is a reasonable inference that Avigilon has had knowledge of the ’566 and ’964 Patents prior to the filing of this Complaint. Plaintiff asserts that this reasonable inference is true.

20. JDS and Avigilon both regularly attend industry trade shows and have done so for several years. Upon information and belief, employees or associates of Avigilon have visited JDS’s display at trade shows including ISC West, ISC East, and ASIS. At the trade shows, JDS prominently displays its products and the patent numbers of the ’566 and ’964 Patents in its materials. It is, therefore, reasonable to

infer that Avigilon has had knowledge of the Patents-in-Suit prior to the filing of the Complaint in this lawsuit. Plaintiff asserts that this reasonable inference is true.

21. Avigilon has knowledge of Plaintiff's video management software and Plaintiff's patents and has for several years.

22. On May 24, 2012, JDS filed a lawsuit for patent infringement against Milestone Systems, Inc. and its parent company Milestone Systems A/S (collectively "Milestone"). Milestone is a direct competitor of both JDS and Avigilon. The lawsuit involved both the '566 and '964 Patents and obtained a fair amount of press coverage in the industry throughout the course of the litigation. Accordingly, Plaintiff hereby asserts that it is a reasonable inference that Avigilon had knowledge of the '566 and '964 Patents prior to the filing of this Complaint. Plaintiff asserts that this reasonable inference is true.

23. Avigilon manufactures, imports, offers for sale, uses, and sells software and systems that infringe claims of the Patents-in-Suit.

V. COUNT I – DIRECT INFRINGEMENT OF USPN 6,891,566

24. Plaintiff repeats and re-alleges the allegations contained in Paragraphs 1-23 above as if fully set forth herein.

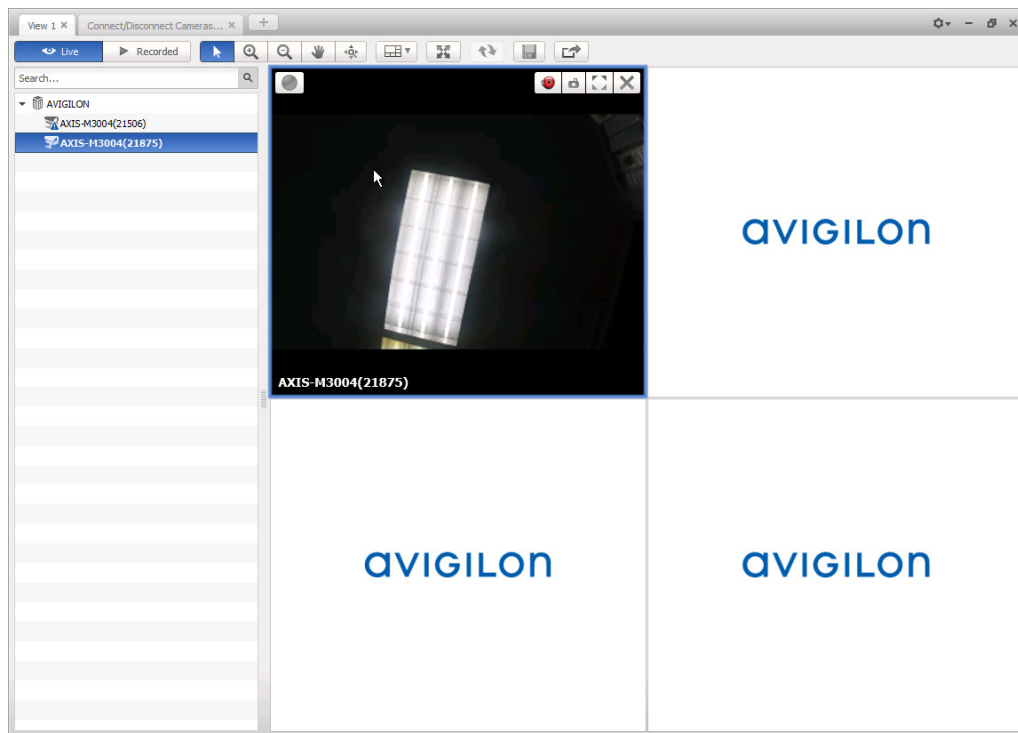
25. Avigilon has made, used, offered for sale, and sold in the United States, and continues to make, use, offer for sale, and sell in the United States video

surveillance software, systems, and components. Avigilon's activities infringe, induce others to infringe, and/or contributorily infringe the '566 Patent. These activities include providing the Avigilon Control Center video management software to customers and instructing customers regarding use of the software. As a non-limiting example, upon information and belief, Kettering University in Flint, Michigan, is one of those customers. By making, using, offering for sale, and/or selling technology including, but not limited to, its Control Center video management software in the United States, Avigilon is infringing claims of the '566 Patent under 35 U.S.C. § 271(a).

26. Claim 1 of the '566 Patent recites the following: "A computer readable medium for use by a computer in providing an interface to multiple cameras via one or more video servers accessible to the computer via a network, comprising: a digital storage device; a user interface program stored on said digital storage device in computer readable form, said program being operable upon execution by the computer to access server data uniquely identifying each video server and to attempt access to the video servers over the network, said program also being operable to obtain from each of the accessible video servers a hardware address stored in the video server; wherein said program is further operable to validate the hardware addresses received from the video servers using the server data and, for those video servers having valid hardware address, said program is operable to generate a user

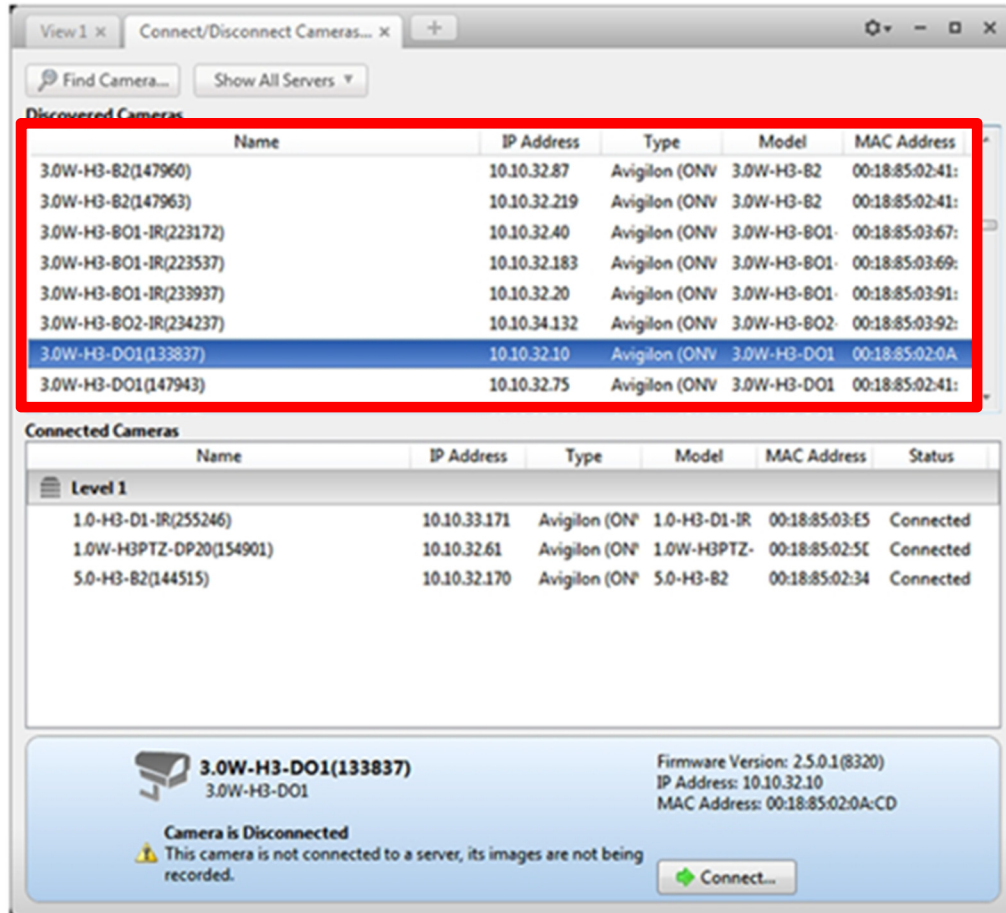
interface display on the computer that includes a display window for each of the cameras accessed via the validated servers over the network and to display in each of the display windows an image received from the camera associated with that display window.”

27. Avigilon’s Control Center software, which resides on Avigilon’s server(s) and can be installed on a user’s computer, is made up of a number of components. Such components include, among others, the “Control Center Server,” the “Control Center Client,” and the “Control Center Player.” Each of these components includes user interfaces. The user interface associated with the Control Center Client application is shown below.



User Interface – Avigilon Control Center Client

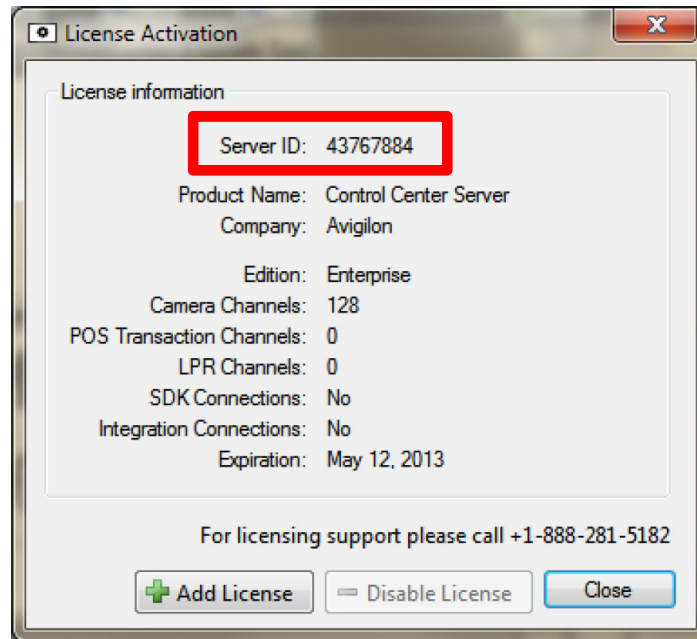
28. During operation, Avigilon's Control Center software accesses data uniquely identifying each video server available over a network, as shown on page 31 of the Client User Guide associated with Avigilon's Control Center software (hereinafter "ACC Client User Guide"), which is reproduced below.



(ACC Client User Guide, p. 31)

29. The Avigilon Control Center software also identifies each server, to which one or more cameras and/or camera servers may be connected, with a particular "Server ID." This is illustrated on page 9 of the Server User Guide associated with Avigilon's Control Center software (hereinafter "ACC Server User

Guide”), which is reproduced below. As explained in the ACC Server User Guide, “The Server ID is unique to each server running the Avigilon Control Center software.” ACC Server User Guide, p. 9.



(ACC Server User Guide, p. 9)

30. A “software license” is required for each server on which Avigilon’s Control Center software is installed. The server license is associated with each server based on a unique identifier, which may include the server’s unique “Server ID.” The Avigilon Control Center software will not run on a particular server unless a server license has been associated with it—as explained on page 8 of the ACC Server User Guide, shown below.


Licensing the Server

After the Avigilon Control Center Server software has been installed, you must apply your software license to the application or the Control Center Server will not run.

Your server can be licensed for the Core, Standard or Enterprise edition. If you are running the Enterprise edition, this procedure is also used to add integration licenses.

(ACC Server User Guide, p. 8)

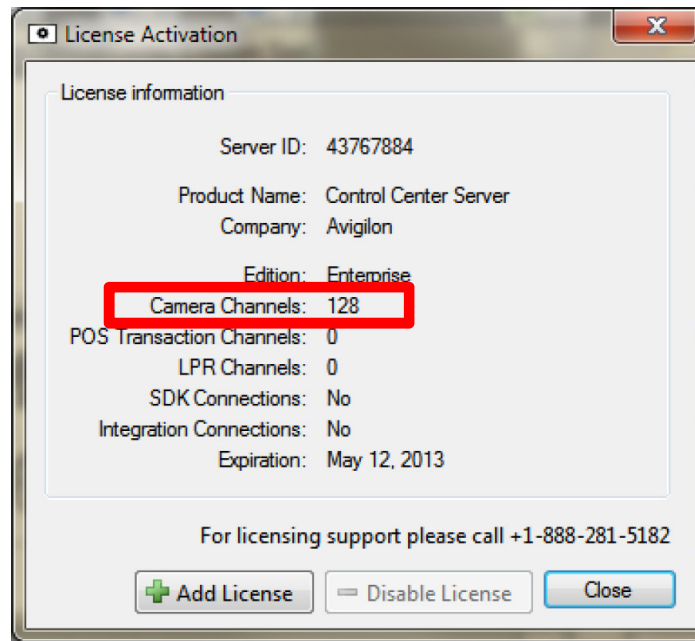
31. Avigilon provides distinct license “editions” that may be associated with each server in a video management system running Avigilon’s Control Center software. The different license editions of the Control Center software currently offered by Avigilon—Core, Standard, and Enterprise—are set forth in the Avigilon Control Center software version 5.2 Data Sheet (hereinafter “ACC Data Sheet”), as illustrated below.



System	Core	Standard	Enterprise
Number of cameras per server	24	48	128
Number of servers per site	1	1	100
Number of concurrent server connections	1	24	Unlimited
Number of client licenses per server	2	5	Unlimited
High Definition Stream Management (HDSM)™	Yes	Yes	Yes
Industry's most powerful VMS engine	Yes	Yes	Yes

(ACC Data Sheet, p. 3)

32. Both the ACC Server User Guide and the ACC Client User Guide further describe how each server license may include a certain number of “Camera Licenses” or “Channel Licenses,” which sets forth the number of cameras that can be operatively connected to each particular server.



(ACC Server User Guide, p. 9)

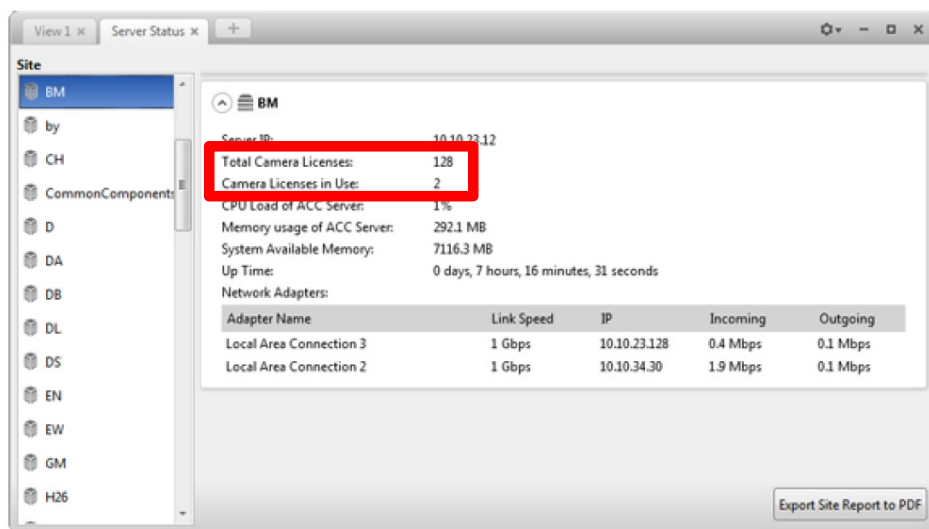


Figure 7: Server Status tab

In the System Explorer, select a Site to display the statuses of connected servers. Listed information includes:

- Server IP: the server's IP address.
- **Total Camera Licenses: the total number of camera channel licenses that have been activated on the server.**
- **Camera Licenses in Use: the number of cameras that are currently connected to the server.**

(ACC Client User Guide, p. 21)

33. Each camera and/or camera server used in a video management system running Avigilon's Control Center software can be assigned a particular "License Priority," which controls the order in which cameras are connected to the server. The "License Priority" and assigned "Camera/Channel License" is associated with each camera and/or camera server based on a unique identifier. Page 32 of the ACC Client User Guide explains the "License Priority" feature of Avigilon's Control Center software:

3. In the Connect Camera dialog box, select the server you want the camera to connect to.

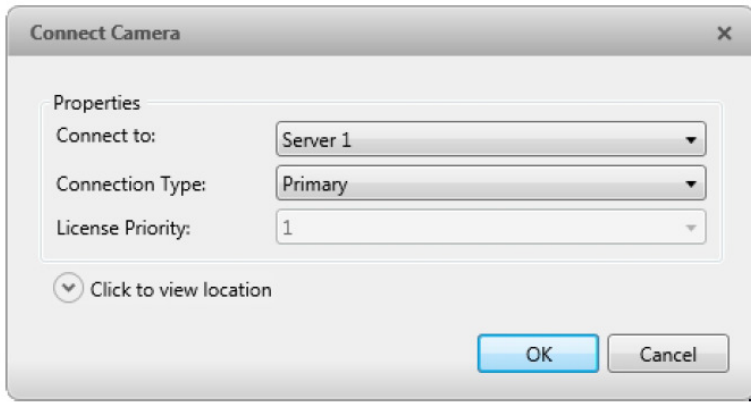


Figure 17: Connect Camera dialog box

4. If you are connecting a third-party camera, you may choose to connect the camera by its native driver. In the **Camera Type:** drop-down list, select the camera's brand name. If there is only one option in the drop-down list, the system only supports one type of driver from the camera.

5. In the **Connection Type:** drop-down list, select **Primary**. The camera will automatically connect to this server if they are in the same network.

If you plan to create failover connections, see [Failover Connections](#) for more information.

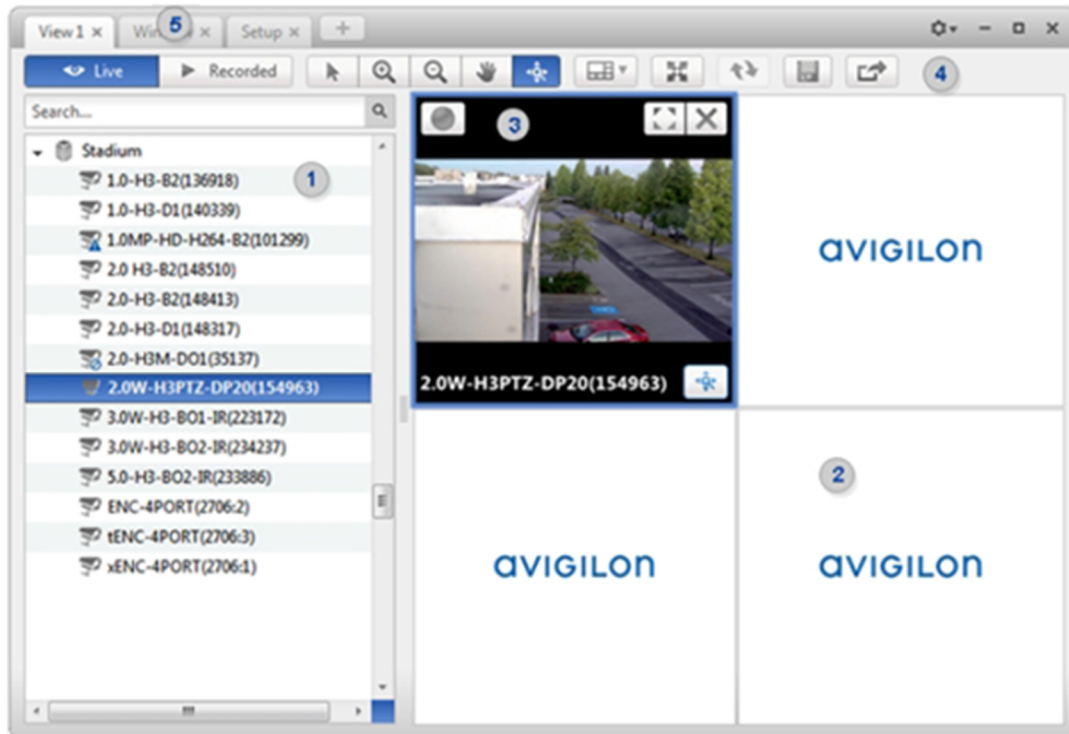
6. In the **License Priority:** drop-down list, select the appropriate license priority. The highest priority is **1** and the lowest priority is **5**.

NOTE: This option is only available if you are connecting to a secondary or tertiary server.

The License Priority: setting decides the order that cameras are connected to the server. The server will try to connect cameras with a higher priority before cameras with lower priority. If the server does not have enough camera channel licenses, low priority cameras may not be connected. A camera channel license is only used when the camera actually connects to the server.

(ACC Client User Guide, p. 32)

34. For licensed cameras and/or servers, Avigilon's Control Center software provides a user interface display on a computer that includes a display window for each of the cameras accessed via the servers over the network, as shown below in an illustration from the ACC Client User Guide.



(ACC Client User Guide, p. 14)

35. The manufacture, use, sale, offer for sale, and importation of Avigilon's Control Center software, the Avigilon Blue Cloud Service software, and the Avigilon hardware with which it is used—including but not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras—directly infringes at least claim 1 of the '566 Patent. Plaintiff has suffered damages as a result of the infringing

activities of Avigilon, and will continue to suffer such damages as long as those infringing activities continue.

36. Avigilon was notified of its infringement of the '566 Patent at least as early as the filing of this Complaint.

37. Avigilon had knowledge of the '566 Patent at least as early as the filing of this Complaint.

38. Upon information and belief, Avigilon has had knowledge of the '566 Patent for several years. Based on the facts alleged above in Paragraphs 18-22, it is reasonable to infer that Avigilon has had knowledge of the '566 Patent since its issuance or since JDS filed suit against Milestone in May of 2012. Alternatively, if Avigilon asserts that it had no knowledge of the '566 Patent prior to the filing of this Complaint, Avigilon was willfully blind to a competitor's patent rights.

39. With knowledge of the '566 Patent, Avigilon continues to infringe the '566 Patent.

40. Avigilon is a substantially larger company than JDS. It would, therefore, be reasonable to infer that Avigilon believed that it could infringe the '566 Patent with impunity based on its size advantage over JDS.

41. It is reasonable to infer based on the facts set forth above in Paragraphs 18-40 above, that Avigilon's conduct has been willful, wanton and deliberate. It is also reasonable to infer that Avigilon's actions have been objectively reckless based

on the facts set forth in Paragraphs 18-40 above. The actions of Avigilon with regard to infringement of the '566 Patent are willful such that Plaintiff is entitled to treble damages under 35 U.S.C. § 284.

42. Plaintiff has suffered damages as a result of the infringing activities of Avigilon and will continue to suffer such damages as long as those infringing activities continue.

43. Plaintiff has no adequate remedy at law. Unless enjoined by this Court, Avigilon will continue such acts of infringement, causing Plaintiff to incur substantial and irreparable damage.

VI. COUNT II – DIRECT INFRINGEMENT OF USPN 8,185,964

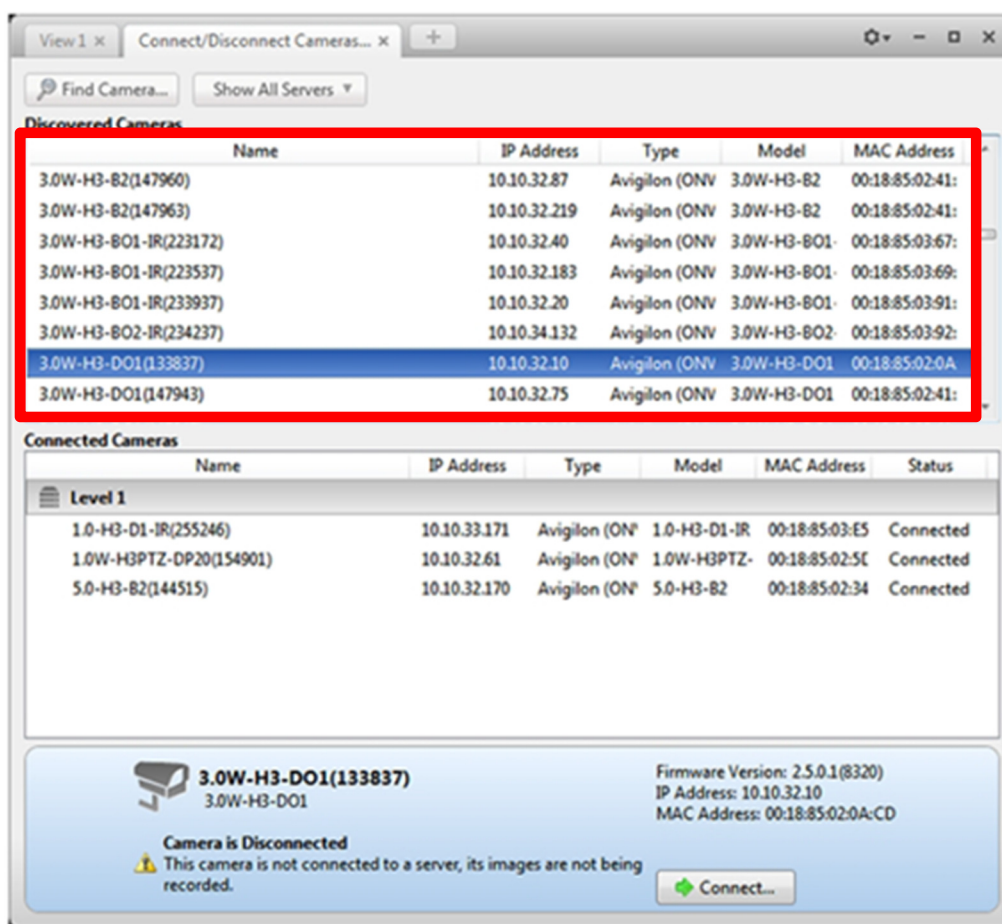
44. Plaintiff repeats and re-alleges the allegations contained in Paragraphs 1-43 above as if fully set forth herein.

45. Avigilon has made, used, offered for sale, and sold in the United States, and continues to make, use, offer for sale, and sell in the United States video surveillance software, systems, and components. Avigilon's activities infringe, induce others to infringe, and/or contributorily infringe the '964 Patent. These activities include providing the Avigilon Control Center video management software to customers and instructing customers regarding use of the software. As a non-limiting example, upon information and belief, Kettering University in Flint, Michigan, is one of those customers. By making, using, offering for sale, and/or selling technology including, but not limited to, its Control Center video management software in the United States, Avigilon is infringing claims of the '964 Patent under 35 U.S.C. § 271(a).

46. Claim 1 of the '964 Patent recites the following: "A method of controlling access by a computer to a video server, comprising the steps of: sending a request from the computer to a video server over a network; receiving at the computer from the video server a unique identifier stored in and identifying the video server, wherein the unique identifier is received by the computer over the network; determining that access to the video server is authorized by comparing the unique

identifier received by the computer to one or more authorized unique identifiers; and in response to the determination, obtaining at the computer one or more images from the video server for displaying.”

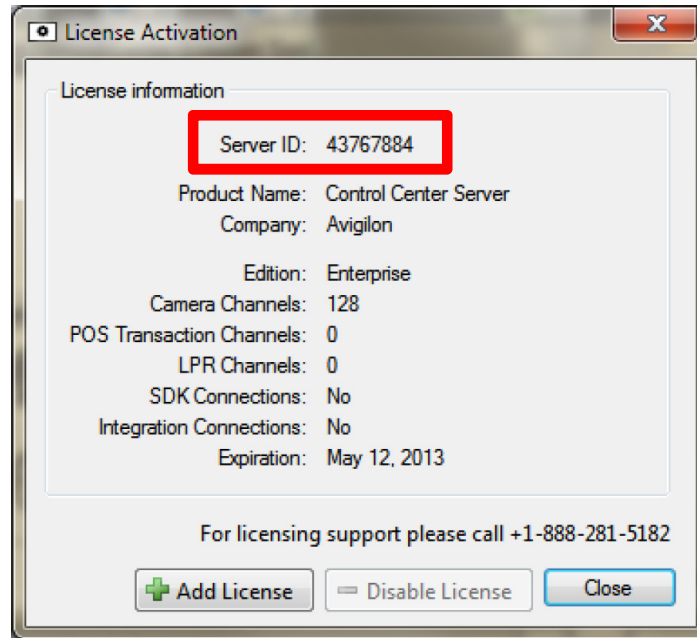
47. During operation, Avigilon’s Control Center software receives information uniquely identifying video servers connected over a network, as shown below.



(ACC Client User Guide, p. 31)

48. The Avigilon Control Center software also identifies each server, to which one or more cameras and/or camera servers may be connected, with a

particular “Server ID.” This is illustrated on page 9 of the ACC Server User Guide, which is reproduced below. As explained in the ACC Server User Guide, “The Server ID is unique to each server running the Avigilon Control Center software.” ACC Server User Guide, p. 9.



(ACC Server User Guide, p. 9)

49. A “software license” is required for each server on which Avigilon’s Control Center software is installed. The server license is associated with each server based on a unique identifier, which may include the server’s unique “Server ID.” The Avigilon Control Center software will not run on a particular server unless a server license has been associated with it—as explained on page 8 of the ACC Server User Guide, shown below.


Licensing the Server

After the Avigilon Control Center Server software has been installed, you must apply your software license to the application or the Control Center Server will not run.

Your server can be licensed for the Core, Standard or Enterprise edition. If you are running the Enterprise edition, this procedure is also used to add integration licenses.

(ACC Server User Guide, p. 8)

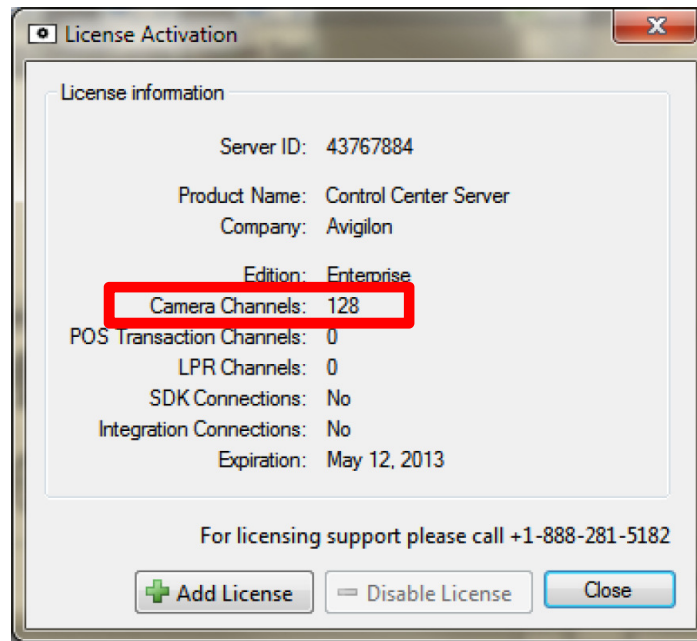
50. Avigilon provides distinct license “editions” that may be associated with each server in a video management system running Avigilon’s Control Center software. The different license editions of the Control Center software currently offered by Avigilon—Core, Standard, and Enterprise—are set forth in the ACC Data Sheet, as illustrated below.



System	Core	Standard	Enterprise
Number of cameras per server	24	48	128
Number of servers per site	1	1	100
Number of concurrent server connections	1	24	Unlimited
Number of client licenses per server	2	5	Unlimited
High Definition Stream Management (HDSM)™	Yes	Yes	Yes
Industry's most powerful VMS engine	Yes	Yes	Yes

(ACC Data Sheet, p. 3)

51. Both the ACC Server User Guide and the ACC Client User Guide further describe how each server license may include a certain number of “Camera Licenses” or “Channel Licenses,” which sets forth the number of cameras that can be operatively connected to each particular server.



(ACC Server User Guide, p. 9)

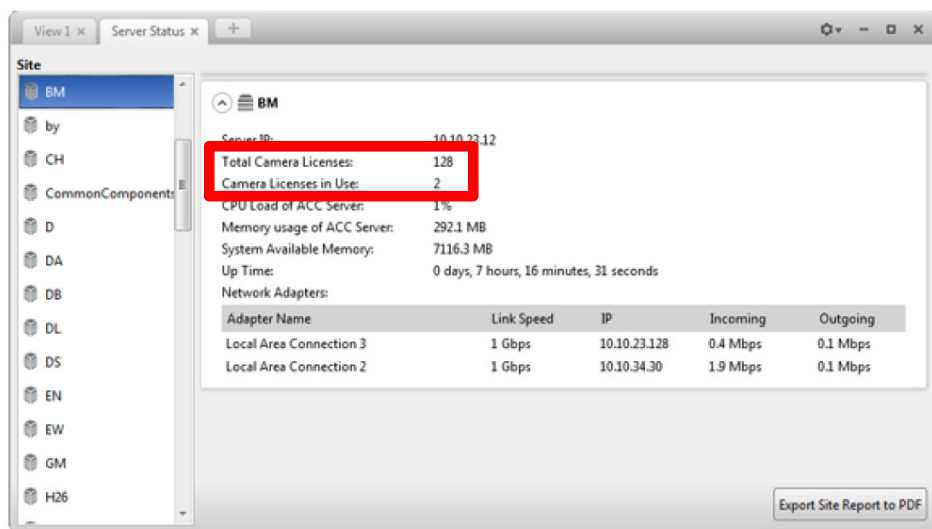


Figure 7: Server Status tab

In the System Explorer, select a Site to display the statuses of connected servers. Listed information includes:

- Server IP: the server's IP address.
- **Total Camera Licenses: the total number of camera channel licenses that have been activated on the server.**
- **Camera Licenses in Use: the number of cameras that are currently connected to the server.**

(ACC Client User Guide, p. 21)

52. Each camera and/or camera server used in a video management system running Avigilon's Control Center software can be assigned a particular "License Priority," which controls the order in which cameras are connected to the server. The "License Priority" and assigned "Camera/Channel License" is associated with each camera and/or camera server based on a unique identifier. Page 32 of the ACC Client User Guide explains the "License Priority" feature of Avigilon's Control Center software:

3. In the Connect Camera dialog box, select the server you want the camera to connect to.

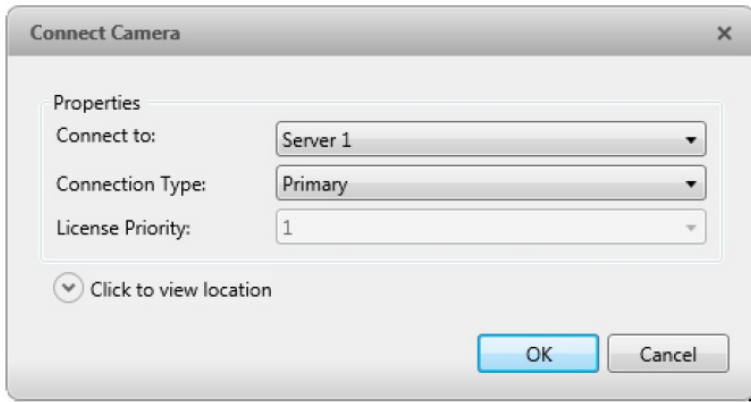


Figure 17: Connect Camera dialog box

4. If you are connecting a third-party camera, you may choose to connect the camera by its native driver. In the **Camera Type:** drop-down list, select the camera's brand name. If there is only one option in the drop-down list, the system only supports one type of driver from the camera.

5. In the **Connection Type:** drop-down list, select **Primary**. The camera will automatically connect to this server if they are in the same network.

If you plan to create failover connections, see [Failover Connections](#) for more information.

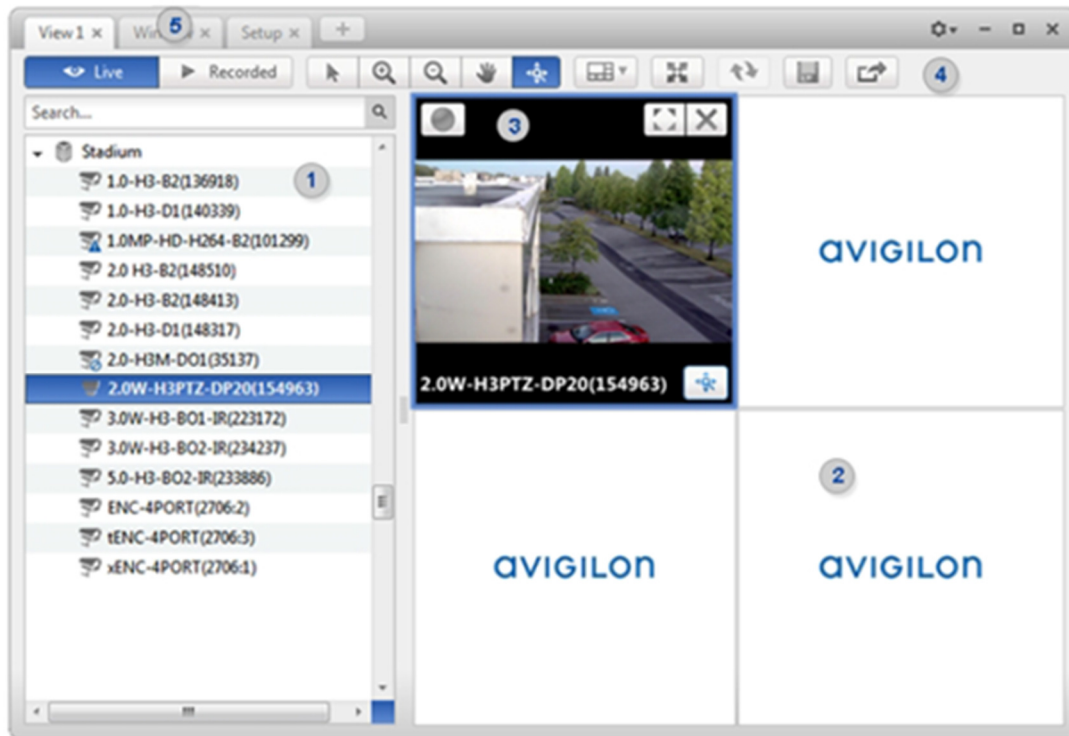
6. In the **License Priority:** drop-down list, select the appropriate license priority. The highest priority is **1** and the lowest priority is **5**.

NOTE: This option is only available if you are connecting to a secondary or tertiary server.

The License Priority: setting decides the order that cameras are connected to the server. The server will try to connect cameras with a higher priority before cameras with lower priority. If the server does not have enough camera channel licenses, low priority cameras may not be connected. A camera channel license is only used when the camera actually connects to the server.

(ACC Client User Guide, p. 32)

53. For licensed cameras and/or servers, Avigilon's Control Center software provides a user interface display for displaying images from the licensed cameras/servers, as shown below in an illustration from the ACC Client User Guide.



(ACC Client User Guide, p. 14)

54. The manufacture, use, sale, offer for sale, and importation of Avigilon's Control Center software, the Avigilon Blue Cloud Service software, and the Avigilon hardware with which it is used—including but not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras—directly infringes at least claim 1 of the '964 Patent. Plaintiff has suffered damages as a result of the infringing activities of Avigilon, and will continue to suffer such damages as long as those infringing activities continue.

55. Avigilon was notified of its infringement of the '964 Patent at least as early as the filing of this Complaint.

56. Avigilon had knowledge of the '964 Patent at least as early as the filing of this Complaint.

57. Upon information and belief, Avigilon has had knowledge of the '964 Patent for several years. Based on the facts alleged above in Paragraphs 18-22, it is reasonable to infer that Avigilon has had knowledge of the '964 Patent since its issuance or since JDS filed suit against Milestone in May of 2012. Alternatively, if Avigilon asserts that it had no knowledge of the '964 Patent prior to the filing of this Complaint, Avigilon was willfully blind to a competitor's patent rights.

58. With knowledge of the '964 Patent, Avigilon continues to infringe the '964 Patent.

59. Avigilon is a substantially larger company than JDS. It would, therefore, be reasonable to infer that Avigilon believed that it could infringe the '964 Patent with impunity based on its size advantage over JDS.

60. It is reasonable to infer based on the facts set forth above in Paragraphs 18-22 and 44-59 above, that Avigilon's conduct has been willful, wanton and deliberate. It is also reasonable to infer that Avigilon's actions have been objectively reckless based on the facts set forth in Paragraphs 18-22 and 44-59 above. The

actions of Avigilon with regard to infringement of the '964 Patent are willful such that Plaintiff is entitled to treble damages under 35 U.S.C. § 284.

61. Plaintiff has suffered damages as a result of the infringing activities of Avigilon and will continue to suffer such damages as long as those infringing activities continue.

62. Plaintiff has no adequate remedy at law. Unless enjoined by this Court, Avigilon will continue such acts of infringement, causing Plaintiff to incur substantial and irreparable damage.

VII.COUNT III – INDIRECT INFRINGEMENT OF USPN 6,891,566

63. Plaintiff repeats and re-alleges the allegations contained in Paragraphs 1-62 above as if fully set forth herein.

64. Claim 49 of the '566 Patent is directed to video management software installed on a computer with cameras connected to the computer.

65. In order for any video management software to provide any intended function, it must be installed on a computer, which is connected—or otherwise has access—to cameras. As shown below, Avigilon states on the data sheet associated with its Control Center software that “Avigilon Control Center can be pre-installed and configured on an Avigilon™ Network Video Recorder (NVR) or work as stand-alone software, to meet the needs of any type of installation.” ACC Data Sheet, p.

1.



(ACC Data Sheet, p. 1)

66. Avigilon's Control Center software is made up of a number of components. Such components include, among others, the "Control Center Server" and the "Control Center Client." As explained on page 10 of the ACC Client User Guide, the Control Center Client software works with the Control Center Server software to provide the user with control of the Avigilon surveillance system.

What is the Avigilon™ Control Center Client?

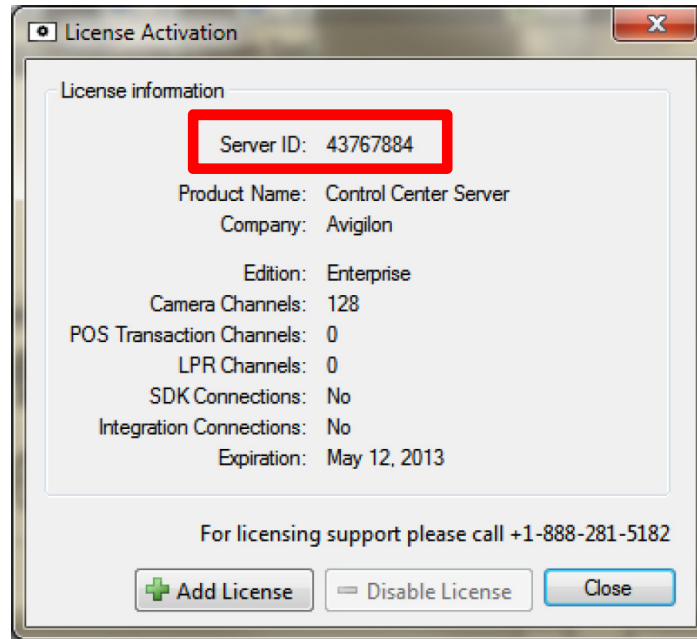
The Avigilon™ Control Center Client software works with the Avigilon™ Control Center Server software to give you access and control of your Avigilon High Definition Stream Management (HDSM)™ surveillance system.

The Client software allows you to view live and recorded video, monitor events, and control user access to the Control Center. The Client software also gives you the ability to configure your surveillance system.

The Client software can run on the same computer as the Server software, or run on a remote computer that connects to the Site through a local area network (LAN) or a wireless area network (WAN).

(ACC Client User Guide, p. 10)

67. The Avigilon Control Center software identifies each server, to which one or more cameras and/or camera servers may be connected, with a particular "Server ID." This is illustrated on page 9 of the ACC Server User Guide, which is reproduced below. As explained in the ACC Server User Guide, "The Server ID is unique to each server running the Avigilon Control Center software." ACC Server User Guide, p. 9.



(ACC Server User Guide, p. 9)

68. A “software license” is required for each server on which Avigilon’s Control Center software is installed. The server license is associated with each server based on a unique number, which may include the server’s unique “Server ID.” The Avigilon Control Center software will not run on a particular server unless a server license has been associated with it—as explained on page 8 of the ACC Server User Guide, shown below.


Licensing the Server

After the Avigilon Control Center Server software has been installed, you must apply your software license to the application or the Control Center Server will not run.

Your server can be licensed for the Core, Standard or Enterprise edition. If you are running the Enterprise edition, this procedure is also used to add integration licenses.

(ACC Server User Guide, p. 8)

69. Avigilon provides distinct license “editions” that may be associated with each server in a video management system running Avigilon’s Control Center software. Each of the different license editions of the Control Center software—Core, Standard, and Enterprise—allows for a different number of camera connections per server, as shown below.



System	Core	Standard	Enterprise
Number of cameras per server	24	48	128
Number of servers per site	1	1	100
Number of concurrent server connections	1	24	Unlimited
Number of client licenses per server	2	5	Unlimited
High Definition Stream Management (HDSM) [™]	Yes	Yes	Yes
Industry's most powerful VMS engine	Yes	Yes	Yes

(ACC Data Sheet, p. 3)

70. In view of the facts alleged above in Paragraphs 63-69, a video management system based on Avigilon’s Control Center software cannot function for its intended purpose without practicing the claims of the ’566 Patent. It is thus a reasonable inference that the Avigilon Control Center software is useless without infringing the ’566 Patent. Plaintiff asserts that this reasonable inference is true.

71. On its website, www.avigilon.com, Avigilon provides download links and instructions for users to install its Control Center software on a computer.

Name	Version	Release Date	Release Notes	Installer
ACC Server 5	5.2.2.24	2014-09-15	Download (pdf) (374 KB)	Download install file (532 MB)
ACC Client 5	5.2.2.24	2014-09-15	Download (pdf) (374 KB)	Download install file (229 MB)
ACC Player 5	5.2.2.24	2014-09-15	Download (pdf) (374 KB)	Download install file (103 MB)
ACC Gateway 5	5.2.2.24	2014-09-15	Download (pdf) (374 KB)	Download install file (96.5 MB)
ACC Virtual Matrix 5	5.2.2.24	2014-09-15	Download (pdf) (374 KB)	Download install file (101 MB)
Camera Installation Tool	4.12.0.48	2014-06-27	Download (pdf) (195 KB)	Download install file (200 MB)

(<http://avigilon.com/support-and-downloads/for-software/software-updates-and-downloads/>)

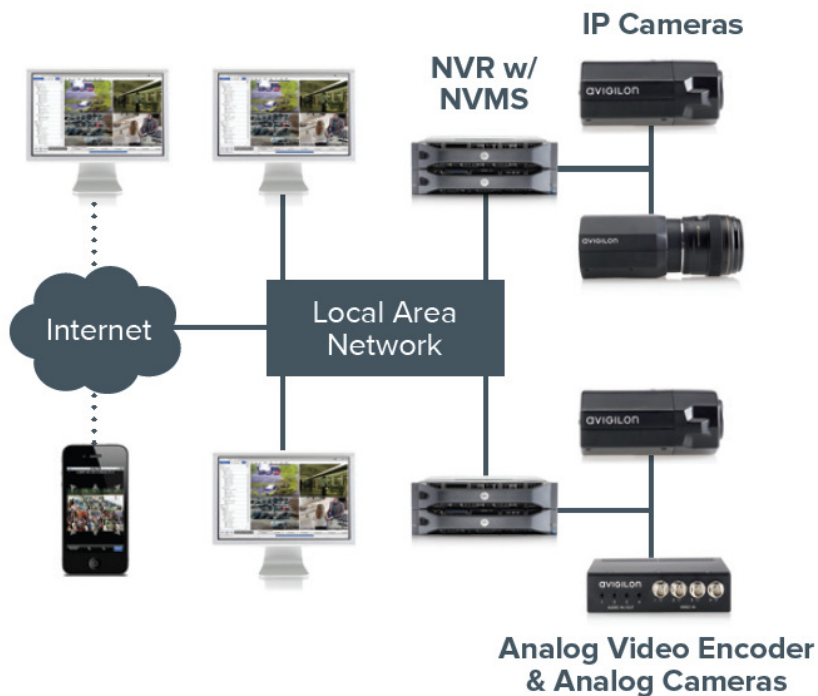
72. During operation, a user is directed and required by Avigilon's Control Center software to install and license a server and associated camera(s) prior to any use of the software. Indeed, claim 49 of the '566 Patent is practiced in this set up procedure mandated and required by Avigilon.

73. Avigilon's website also states that it provides "Industry-leading service and support" for its partners and end users. See <http://avigilon.com/support-and-downloads/>. Avigilon also makes available a number of "Training & How-To videos" related to installation and use of its Control Center software. *Id.*

74. On its website, Avigilon presents numerous "Case Studies." See <http://avigilon.com/case-studies/>. As expected, these studies illustrate that Avigilon's software is to be installed on a computer and connected to cameras at each customer location. As an example, Avigilon states that Prairie Meadows

Racetrack Casino Hotel has a system of hundreds of Avigilon cameras and encoders, which “is monitored live 24x7, 365 days a year using the Avigilon Control Center (ACC) network video management software (NVMS) and 30 Avigilon HD Network Video Recorders (NVRs), which stores at minimum 7 days of continuous footage of the gaming floor and all other areas.” *See* <http://avigilon.com/case-studies/prairie-meadows-racetrack-casino-hotel/>.

75. On the data sheet associated with its Control Center software—and also on its website and many of the informational documents and instructional materials it makes available through its website—Avigilon illustrates how its software must be installed on a computer and connected to cameras to provide its intended function as video management software.



(ACC Data Sheet, p. 2)

76. Avigilon's Control Center video management software has no substantial non-infringing uses other than use with a computer and connected to cameras. Indeed, software has no use if not installed on a computer. And video management software has no use without being connected to a source of video, *i.e.*, a camera and servers. In order to use Avigilon's software to provide any intended use, the claims of the '566 Patent are practiced.

77. The reasonable inference drawn from the facts set forth above in Paragraphs 63-76 is that Avigilon's Control Center software is a material part of the system claimed in the '566 Patent and that it is not a staple item of commerce. Avigilon's Control Center software has no use without infringing the '566 Patent. Plaintiff asserts that this reasonable inference is true.

78. Another reasonable inference from the facts set forth above is that Avigilon knowingly and actively induced—and continues to induce—its customers to install its Control Center software on a computer with connected servers and cameras. Avigilon knowingly and actively requires its customers to infringe the '566 Patent. Plaintiff asserts that this reasonable inference is true.

79. Avigilon's customers directly infringe the '566 Patent by their use of the Avigilon Control Center software on computers connected to servers and cameras. As stated above, upon information and belief, St. Joseph Mercy Oakland

Hospital is one of those customers. Avigilon's other customers that directly infringe the '566 Patent are too numerous to identify by name.

80. Claim 49 of the '566 Patent recites the following: "A digital video system, comprising: a client computer, one or more video servers accessible by the client computer over a network; a plurality of cameras connected to the video server(s), said video server(s) providing an interface between the cameras and client computer in which images from the cameras are accessed by the video server(s) and then sent to the client computer upon request by the client computer; the video server(s) including a unique number that is stored in memory within the video server(s) and that is accessible to the client computer over the network; wherein the client computer provides a user interface display on the computer that includes a display window for each of the cameras accessed over the network and that displays in each of the display windows an image received from the camera associated with that display window; and wherein the client computer uses the unique number obtained from a particular video server to determine whether to enable or disable the display of images from one or more cameras connected to that particular video server."

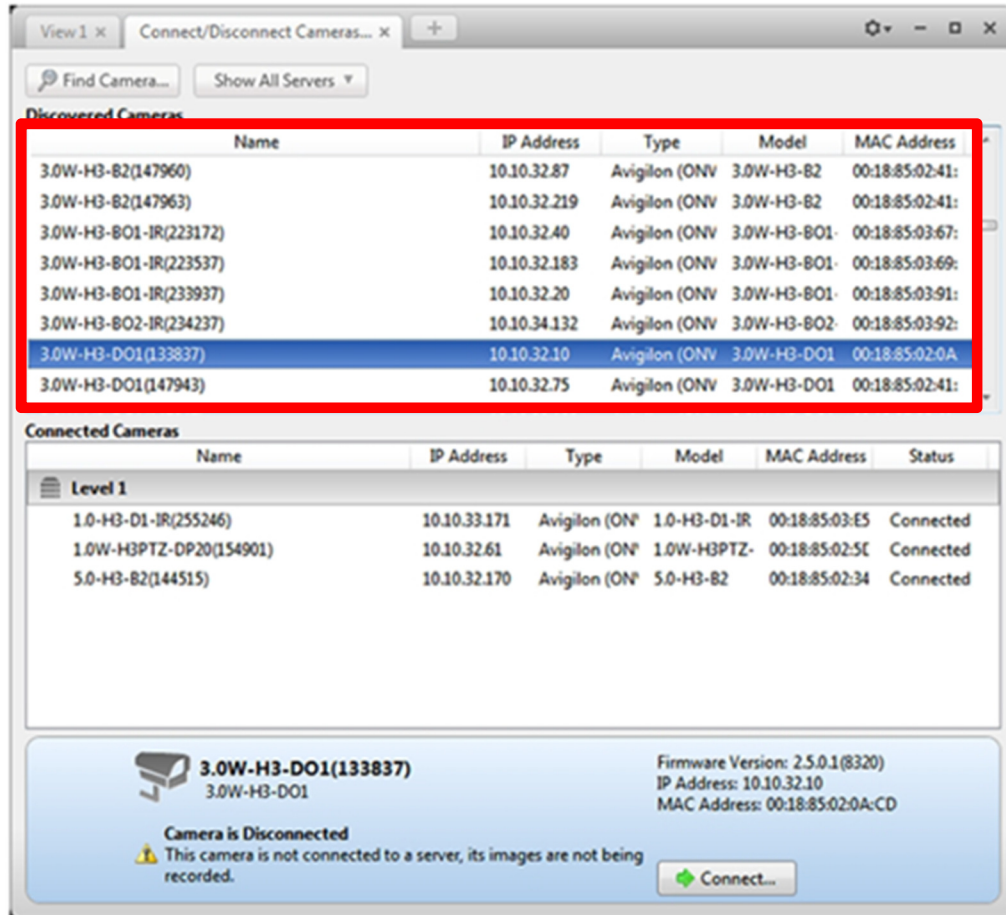
81. Prior to any use of Avigilon's software, it must be installed on a computer as described above.

82. Prior to any use of Avigilon's Control Center software for its intended function, the user is instructed to add and license associated servers and connected cameras. *See, e.g.*, ACC Server User Guide, pp. 8-23 and ACC Client User Guide, pp. 28-33.

83. Prior to any use of Avigilon's Control Center software for its intended function, the software ensures that one or more video servers are made accessible over a network. A unique number associated with the video server is accessible by Avigilon's software.

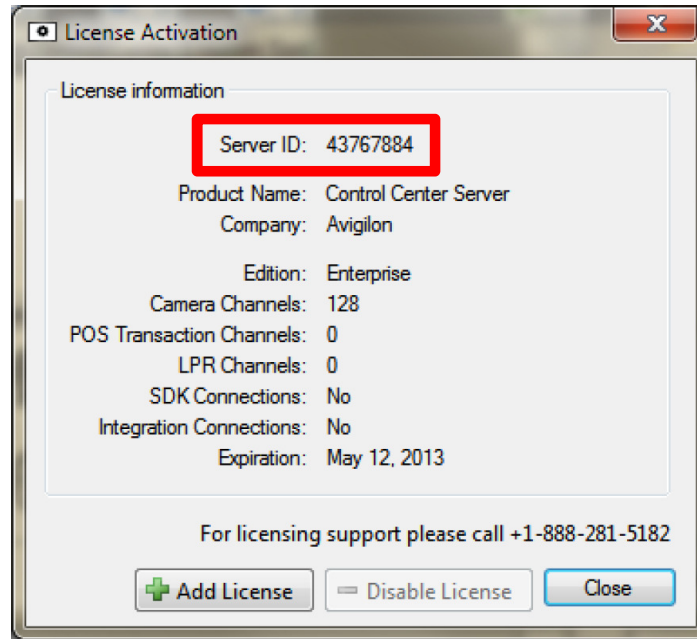
84. Prior to any use of Avigilon's Control Center software for its intended function, the user is instructed to add hardware devices that are connected to the computer via a network and are thus accessible to the software. Each camera or server includes a unique number stored in memory that Avigilon's Control Center software obtains prior to any use of the system to display images from the cameras, as illustrated and described in Paragraphs 24-43 above.

85. The Client User Guide associated with Avigilon's Control Center software illustrates that operation of the software allows a client computer to access a unique number associated with connected cameras.



(ACC Client User Guide, p. 31)

86. Similarly, the Server User Guide associated with Avigilon's Control Center software illustrates that operation of the software allows a client computer to access a unique number associated with connected servers.



(ACC Server User Guide, p. 9)

87. Avigilon's Control Center software uses the unique number associated with a particular server to determine whether to enable or disable the display of images from one or more connected cameras. Page 8 of the ACC Server User Guide, shown below, explains that a license must be applied for the Avigilon Control Center software to run on a particular server.

Licensing the Server

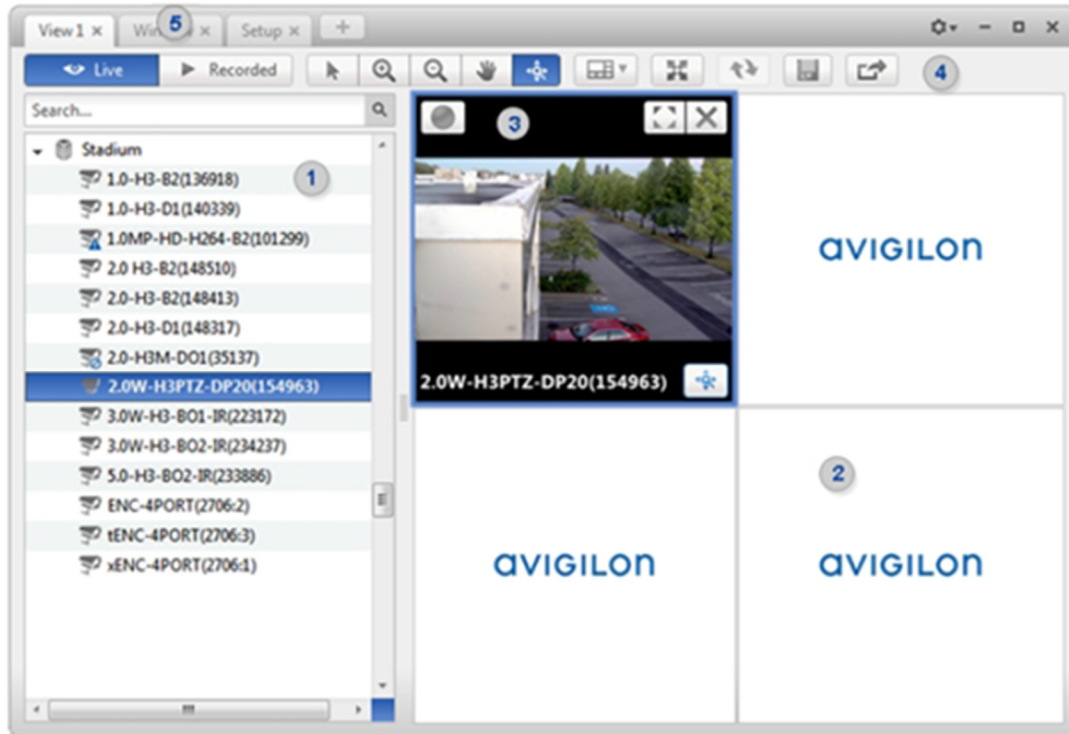
After the Avigilon Control Center Server software has been installed, you must apply your software license to the application or the Control Center Server will not run.

Your server can be licensed for the Core, Standard or Enterprise edition. If you are running the Enterprise edition, this procedure is also used to add integration licenses.

(ACC Server User Guide, p. 8)

88. For licensed cameras and/or servers, Avigilon's Control Center software provides a user interface display on a computer that includes a display

window for each of the cameras accessed via the servers over the network, as shown below in an illustration from the ACC Client User Guide.



(ACC Client User Guide, p. 14)

89. Avigilon's Control Center software is a material part of the system claimed in claim 49 of the '566 Patent. Avigilon's Control Center software, like all software, is required to be installed on a computer. Specifically, in order to use Avigilon's Control Center software for the accessing and displaying of camera images (which is the purpose of the software) it must be installed on a computer connected to cameras. The Avigilon video management software manages and dictates the interaction between these devices as set forth in claim 49.

90. As set forth above, Avigilon's Control Center software has no substantial non-infringing use and is not a staple article of commerce. Without infringing, the software is not permitted to access and view images from cameras—its sole use.

91. Based on the facts alleged above, it is a reasonable inference that Avigilon knew that its software was especially made or adapted for use to infringe the '566 Patent when it sells its Control Center software.

92. Plaintiff has suffered damages as a result of the infringing activities of Avigilon, and will continue to suffer such damages as long as those infringing activities continue.

93. Avigilon had knowledge of the '566 Patent at least as early as the filing of this Complaint.

94. Upon information and belief, Avigilon has had knowledge of the '566 Patent for several years. Based on the facts alleged above in Paragraphs 18-22, it is reasonable to infer that Avigilon has had knowledge of the '566 Patent since its issuance or since JDS filed suit against Milestone in May of 2012. Alternatively, if Avigilon asserts that it had no knowledge of the '566 Patent prior to the filing of this Complaint, Avigilon was willfully blind to a competitor's patent rights.

95. After knowledge of the '566 Patent, Avigilon continues to infringe the '566 Patent by its sale of Control Center software. After knowledge of the '566

Patent, Avigilon continues to take active steps to market, sell, instruct and support to customers and potential customers of Avigilon's Control Center software to infringe the '566 Patent. After knowledge of the '566 Patent, Avigilon continues to advertise on its website its Control Center software used specifically in combination with a computer and cameras in practicing the '566 Patent.

96. It is reasonable to infer based on the facts set forth above in Paragraphs 63-95, that Avigilon knowingly and affirmatively intends to actively induce and contribute to the infringement of the '566 Patent. Plaintiff asserts that this reasonable inference is true.

97. Avigilon has made, used, offered for sale, and sold in the United States, and continues to make, use, offer for sale, and sell in the United States video surveillance software and systems. Avigilon's activities contributorily infringe the '566 Patent. These activities include selling the Avigilon Control Center software, the Avigilon Blue Cloud Service software, and the Avigilon hardware with which it is used—including but not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras—to partners and/or customers. By making, using, offering for sale and selling technology including, but not limited to, its Control Center software in the United States, Avigilon is infringing claims of the '566 Patent under 35 U.S.C. § 271(c).

98. Avigilon has made, used, offered for sale, and sold in the United States, and continues to make, use, offer for sale, and sell in the United States video surveillance software and systems. Avigilon's activities induce infringement the '566 Patent. These activities include selling the Avigilon Control Center software, the Avigilon Blue Cloud Service software, and the Avigilon hardware with which it is used—including but not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras—to partners and/or customers, requiring, instructing and supporting their use to infringe the '566 Patent, and designing the software so that the only use of the software is to infringe the '566 Patent. Avigilon is infringing claims of the '566 Patent under 35 U.S.C. § 271(b).

99. It is reasonable to infer based on the facts set forth above in Paragraphs 18-40, that Avigilon's conduct has been willful, wanton and deliberate. It is also reasonable to infer that Avigilon's actions have been objectively reckless based on the facts set forth in Paragraphs 18-40 above. The actions of Avigilon with regard to infringement of the '566 Patent are willful such that JDS is entitled to treble damages under 35 U.S.C. § 284.

100. After knowledge of the '566 Patent, Avigilon continues to infringe the '566 Patent.

101. Avigilon is a substantially larger company than JDS. It would, therefore, be reasonable to infer that Avigilon believed that it could infringe the '566 Patent with impunity based on its size advantage over JDS.

102. Plaintiff has suffered damages as a result of the infringing activities of Avigilon, and will continue to suffer damages as long as those infringing activities continue.

103. Plaintiff has no adequate remedy at law. Unless enjoined by this Court, Avigilon will continue such willful acts of infringement, causing Plaintiff to incur substantial and irreparable damages.

VIII. COUNT IV – INDIRECT INFRINGEMENT OF USPN 8,185,964

104. Plaintiff repeats and re-allege the allegations contained in Paragraphs 1-103 above as if fully set forth herein

105. Claim 1 of the '964 Patent is directed to method of using video management software installed on a computer with cameras connected to the computer.

106. In order for any video management software to provide any intended function, it must be installed on a computer, which is connected—or otherwise has access—to cameras. As shown below, Avigilon states on the data sheet associated with its Control Center software that “Avigilon Control Center can be pre-installed and configured on an Avigilon™ Network Video Recorder (NVR) or work as stand-alone software, to meet the needs of any type of installation.” ACC Data Sheet, p. 1.



(ACC Data Sheet, p. 1)

107. Avigilon's Control Center software is made up of a number of components. Such components include, among others, the "Control Center Server" and the "Control Center Client." As explained on page 10 of the ACC Client User Guide, the Control Center Client software works with the Control Center Server software to provide the user with control of the Avigilon surveillance system.

What is the Avigilon™ Control Center Client?

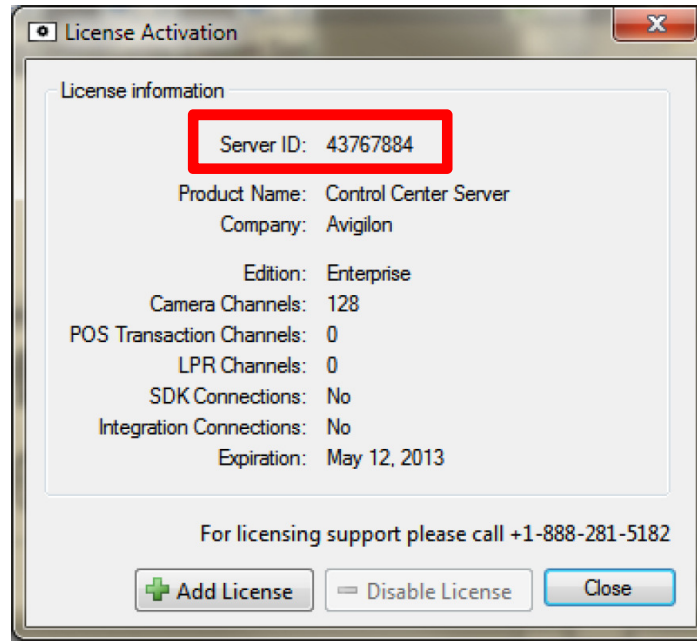
The Avigilon™ Control Center Client software works with the Avigilon™ Control Center Server software to give you access and control of your Avigilon High Definition Stream Management (HDSM)™ surveillance system.

The Client software allows you to view live and recorded video, monitor events, and control user access to the Control Center. The Client software also gives you the ability to configure your surveillance system.

The Client software can run on the same computer as the Server software, or run on a remote computer that connects to the Site through a local area network (LAN) or a wireless area network (WAN).

(ACC Client User Guide, p. 10)

108. The Avigilon Control Center software identifies each server, to which one or more cameras and/or camera servers may be connected, with a particular "Server ID." This is illustrated on page 9 of the ACC Server User Guide, which is reproduced below. As explained in the ACC Server User Guide, "The Server ID is unique to each server running the Avigilon Control Center software." ACC Server User Guide, p. 9.



(ACC Server User Guide, p. 9)

109. A “software license” is required for each server on which Avigilon’s Control Center software is installed. The server license is associated with each server based on a unique identifier, which may include the server’s unique “Server ID.” The Avigilon Control Center software will not run on a particular server unless a server license has been associated with it—as explained on page 8 of the ACC Server User Guide, shown below.


Licensing the Server

After the Avigilon Control Center Server software has been installed, you must apply your software license to the application or the Control Center Server will not run.

Your server can be licensed for the Core, Standard or Enterprise edition. If you are running the Enterprise edition, this procedure is also used to add integration licenses.

(ACC Server User Guide, p. 8)

110. Avigilon provides distinct license “editions” that may be associated with each server in a video management system running Avigilon’s Control Center software. Each of the different license editions of the Control Center software—Core, Standard, and Enterprise—allows for a different number of camera connections per server, as shown below.



System	Core	Standard	Enterprise
Number of cameras per server	24	48	128
Number of servers per site	1	1	100
Number of concurrent server connections	1	24	Unlimited
Number of client licenses per server	2	5	Unlimited
High Definition Stream Management (HDSM) [™]	Yes	Yes	Yes
Industry's most powerful VMS engine	Yes	Yes	Yes

(ACC Data Sheet, p. 3)

111. In view of the facts alleged above in Paragraphs 104-110, a video management system based on Avigilon’s Control Center software cannot function for its intended purpose without practicing the claims of the ’964 Patent. It is thus a reasonable inference that the Avigilon Control Center software is useless without infringing the ’964 Patent. Plaintiff asserts that this reasonable inference is true.

112. On its website, www.avigilon.com, Avigilon provides download links and instructions for users to install its Control Center software on a computer.

Name	Version	Release Date	Release Notes	Installer
ACC Server 5	5.2.2.24	2014-09-15	Download (pdf) (374 KB)	Download install file (532 MB)
ACC Client 5	5.2.2.24	2014-09-15	Download (pdf) (374 KB)	Download install file (229 MB)
ACC Player 5	5.2.2.24	2014-09-15	Download (pdf) (374 KB)	Download install file (103 MB)
ACC Gateway 5	5.2.2.24	2014-09-15	Download (pdf) (374 KB)	Download install file (96.5 MB)
ACC Virtual Matrix 5	5.2.2.24	2014-09-15	Download (pdf) (374 KB)	Download install file (101 MB)
Camera Installation Tool	4.12.0.48	2014-06-27	Download (pdf) (195 KB)	Download install file (200 MB)

(<http://avigilon.com/support-and-downloads/for-software/software-updates-and-downloads/>)

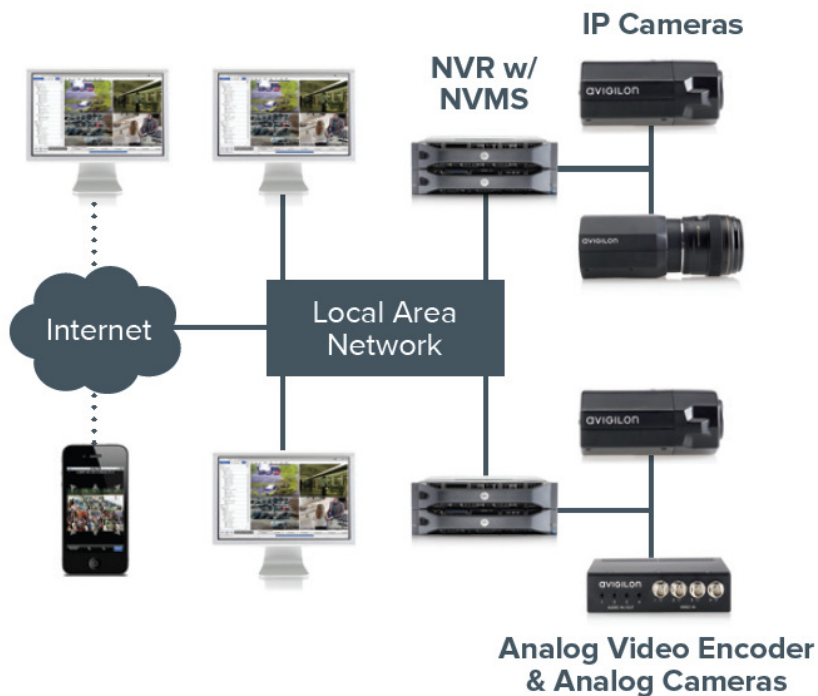
113. During operation, a user is directed and required by Avigilon's Control Center software to install and license a server and associated camera(s) prior to any use of the software. Indeed, claim 1 of the '964 Patent is practiced in this set up procedure mandated and required by Avigilon.

114. Avigilon's website also states that it provides "Industry-leading service and support" for its partners and end users. See <http://avigilon.com/support-and-downloads/>. Avigilon also makes available a number of "Training & How-To videos" related to installation and use of its Control Center software. *Id.*

115. On its website, Avigilon presents numerous "Case Studies." See <http://avigilon.com/case-studies/>. As expected, these studies illustrate that Avigilon's software is to be installed on a computer and connected to cameras at each customer location. As an example, Avigilon states that Prairie Meadows

Racetrack Casino Hotel has a system of hundreds of Avigilon cameras and encoders, which “is monitored live 24x7, 365 days a year using the Avigilon Control Center (ACC) network video management software (NVMS) and 30 Avigilon HD Network Video Recorders (NVRs), which stores at minimum 7 days of continuous footage of the gaming floor and all other areas.” *See* <http://avigilon.com/case-studies/prairie-meadows-racetrack-casino-hotel/>.

116. On the data sheet associated with its Control Center software—and also on its website and many of the informational documents and instructional materials it makes available through its website—Avigilon illustrates how its software must be installed on a computer and connected to cameras to provide its intended function as video management software.



(ACC Data Sheet, p. 2)

117. Avigilon's Control Center video management software has no substantial non-infringing uses other than use with a computer and connected to cameras. Indeed, software has no use if not installed on a computer. And video management software has no use without being connected to a source of video, *i.e.*, a camera and servers. In order to use Avigilon's software to provide any intended use, the claims of the '964 Patent are practiced.

118. The reasonable inference drawn from the facts set forth above in Paragraphs 104-117 is that Avigilon's Control Center software is a material part of the method claimed in the '964 Patent and that it is not a staple item of commerce. Avigilon's Control Center software has no use without infringing the '964 Patent. Plaintiff asserts that this reasonable inference is true.

119. Another reasonable inference from the facts set forth above is that Avigilon knowingly and actively induced—and continues to induce—its customers to install its Control Center software on a computer with connected servers and cameras. Avigilon knowingly and actively requires its customers to infringe the '964 Patent. Plaintiff asserts that this reasonable inference is true.

120. Avigilon's customers directly infringe the '964 Patent by their use of the Avigilon Control Center software on computers connected to servers and cameras. As stated above, upon information and belief, St. Joseph Mercy Oakland

Hospital is one of those customers. Avigilon's other customers that directly infringe the '964 Patent are too numerous to identify by name.

121. Claim 1 of the '964 Patent recites the following: "A method of controlling access by a computer to a video server, comprising the steps of: sending a request from the computer to a video server over a network; receiving at the computer from the video server a unique identifier stored in and identifying the video server, wherein the unique identifier is received by the computer over the network; determining that access to the video server is authorized by comparing the unique identifier received by the computer to one or more authorized unique identifiers; and in response to the determination, obtaining at the computer one or more images from the video server for displaying."

122. Prior to any use of Avigilon's software, it must be installed on a computer as described above.

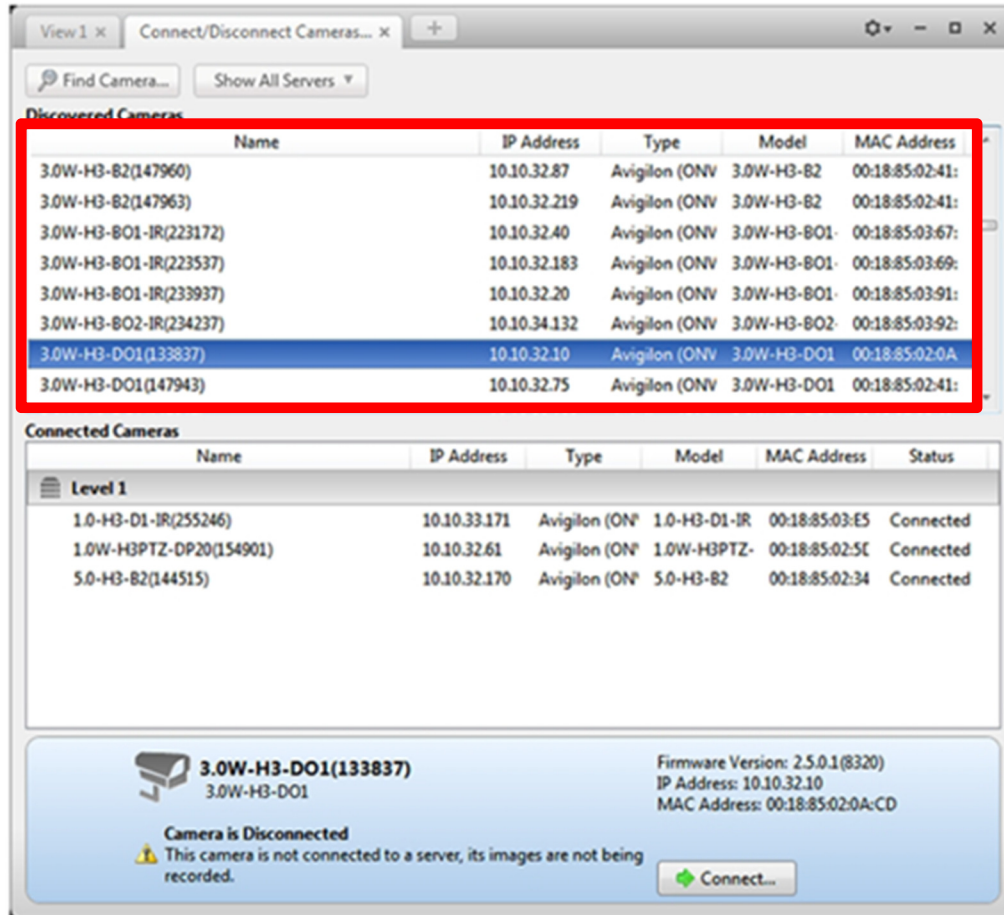
123. Prior to any use of Avigilon's Control Center software for its intended function, the user is instructed to add and license associated servers and connected cameras. *See, e.g.*, ACC Server User Guide, pp. 8-23 and ACC Client User Guide, pp. 28-33.

124. Prior to any use of Avigilon's Control Center software for its intended function, the software ensures that one or more video servers are made accessible

over a network. A unique identifier associated with the video server is accessible by Avigilon's software.

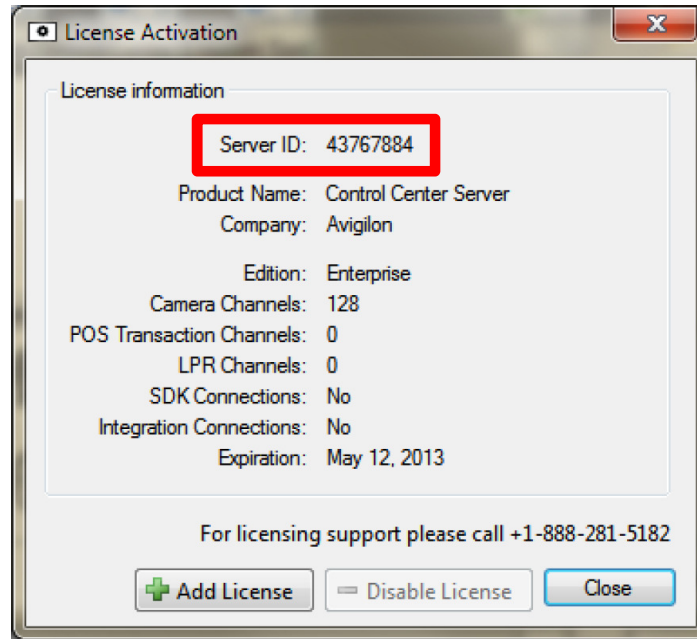
125. Prior to any use of Avigilon's Control Center software for its intended function, the user is instructed to add hardware devices that are connected to the computer via a network and are thus accessible to the software. Each camera or server includes a unique identifier that Avigilon's Control Center software obtains prior to any use of the system to display images from the cameras, as illustrated and described in Paragraphs 44-62 above.

126. The Client User Guide associated with Avigilon's Control Center software illustrates that operation of the software involves receiving a unique identifier associated with connected cameras.



(ACC Client User Guide, p. 31)

127. Similarly, the Server User Guide associated with Avigilon's Control Center software illustrates that operation of the software involves receiving a unique identifier associated with connected servers.



(ACC Server User Guide, p. 9)

128. Avigilon's Control Center software uses the unique identifier associated with a particular server to determine whether access to images from one or more connected cameras is authorized. Page 8 of the ACC Server User Guide, shown below, explains that a license must be applied for the Avigilon Control Center software to run on a particular server.

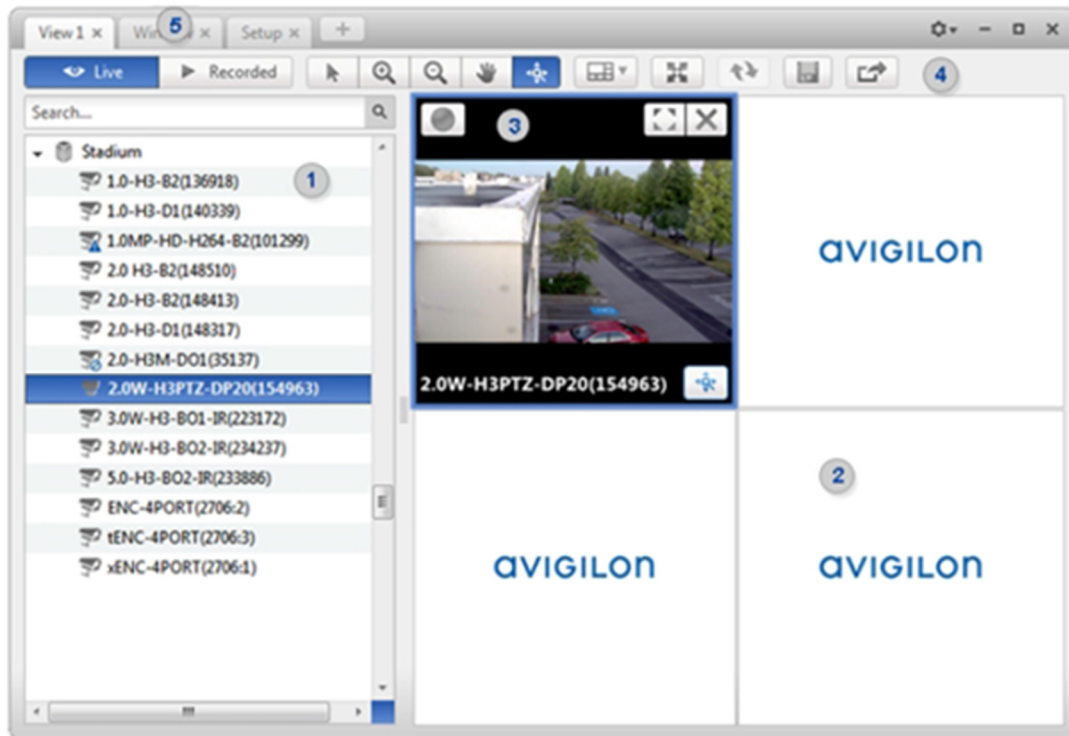
Licensing the Server

After the Avigilon Control Center Server software has been installed, you must apply your software license to the application or the Control Center Server will not run.

Your server can be licensed for the Core, Standard or Enterprise edition. If you are running the Enterprise edition, this procedure is also used to add integration licenses.

(ACC Server User Guide, p. 8)

129. For licensed cameras and/or servers, Avigilon's Control Center software provides a user interface display for displaying images from the licensed cameras/servers, as shown below in an illustration from the ACC Client User Guide.



(ACC Client User Guide, p. 14)

130. Avigilon's Control Center software is a material part of the method claimed in claim 1 of the '964 Patent. Avigilon's Control Center software, like all software, is required to be installed on a computer. Specifically, in order to use Avigilon's Control Center software for the accessing and displaying of camera images (which is the purpose of the software) it must be installed on a computer connected to cameras.

131. As set forth above, Avigilon's Control Center software has no substantial non-infringing use and is not a staple article of commerce. Without infringing, the software is not permitted to access and view images from cameras—its sole use.

132. Based on the facts alleged above, it is a reasonable inference that Avigilon knew that its software was especially made or adapted for use to infringe the '964 Patent when it sells its Control Center software.

133. Plaintiff has suffered damages as a result of the infringing activities of Avigilon, and will continue to suffer such damages as long as those infringing activities continue.

134. Avigilon had knowledge of the '964 Patent at least as early as the filing of this Complaint.

135. Upon information and belief, Avigilon has had knowledge of the '964 Patent for several years. Based on the facts alleged above in Paragraphs 18-22, it is reasonable to infer that Avigilon has had knowledge of the '964 Patent since its issuance or since JDS filed suit against Milestone in May of 2012. Alternatively, if Avigilon asserts that it had no knowledge of the '964 Patent prior to the filing of this Complaint, Avigilon was willfully blind to a competitor's patent rights.

136. After knowledge of the '964 Patent, Avigilon continues to infringe the '964 Patent by its sale of Control Center software. After knowledge of the '964

Patent, Avigilon continues to take active steps to market, sell, instruct and support to customers and potential customers of Avigilon's Control Center software, the Avigilon Blue Cloud Service software, and the Avigilon hardware with which it is used—including but not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras—to infringe the '964 Patent. After knowledge of the '964 Patent, Avigilon continues to advertise on its website its Control Center software used specifically in combination with a computer and cameras in practicing the '964 Patent.

137. It is reasonable to infer based on the facts set forth above in Paragraphs 104-136, that Avigilon knowingly and affirmatively intends to actively induce and contribute to the infringement of the '964 Patent. Plaintiff asserts that this reasonable inference is true.

138. Avigilon has made, used, offered for sale, and sold in the United States, and continues to make, use, offer for sale, and sell in the United States video surveillance software and systems. Avigilon's activities contributorily infringe the '964 Patent. These activities include selling the Avigilon Control Center software, the Avigilon Blue Cloud Service software, and the Avigilon hardware with which it is used—including but not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras—to partners and/or customers. By making, using, offering for sale and selling technology including, but not limited to, its Control Center

software in the United States, Avigilon is infringing claims of the '964 Patent under 35 U.S.C. § 271(c).

139. Avigilon has made, used, offered for sale, and sold in the United States, and continues to make, use, offer for sale, and sell in the United States video surveillance software and systems. Avigilon's activities induce infringement the '964 Patent. These activities include selling the Avigilon Control Center software to partners and/or customers, requiring, instructing and supporting their use to infringe the '964 Patent, and designing the software so that the only use of the software is to infringe the '964 Patent. Avigilon is infringing claims of the '964 Patent under 35 U.S.C. § 271(b).

140. It is reasonable to infer based on the facts set forth above in Paragraphs 18-22 and 44-59, that Avigilon's conduct has been willful, wanton and deliberate. It is also reasonable to infer that Avigilon's actions have been objectively reckless based on the facts set forth in Paragraphs 18-22 and 44-59 above. The actions of Avigilon with regard to infringement of the '964 Patent are willful such that JDS is entitled to treble damages under 35 U.S.C. § 284.

141. After knowledge of the '964 Patent, Avigilon continues to infringe the '964 Patent.

142. Avigilon is a substantially larger company than JDS. It would, therefore, be reasonable to infer that Avigilon believed that it could infringe the '964 Patent with impunity based on its size advantage over JDS.

143. Plaintiff has suffered damages as a result of the infringing activities of Avigilon, and will continue to suffer damages as long as those infringing activities continue.

144. Plaintiff has no adequate remedy at law. Unless enjoined by this Court, Avigilon will continue such willful acts of infringement, causing Plaintiff to incur substantial and irreparable damages.

**IX. COUNT V – INFRINGEMENT OF USPN 6,891,566 UNDER 35
U.S.C. § 271(f)**

145. Plaintiff repeats and re-alleges the allegations contained in Paragraphs 1-144 above as if fully set forth herein.

146. Plaintiff specifically incorporates here each of its allegations in connection with Count III regarding indirect infringement of the '566 Patent, which are set forth in Paragraphs 63-103 above.

147. Avigilon commonly supplies or causes to be supplied in or from the United States all or a substantial portion of the components recited in claims of the '566 Patent. As one example, Avigilon commonly supplies or causes to be supplied

in or from the United States all or a substantial portion of the components recited in claim 49 of the '566 Patent.

148. In circumstances where such components are uncombined in whole or in part, Avigilon supplies these components—including but not limited to software, network video recorders (NVRs), workstations, appliances, encoders, and cameras—in such manner as to actively induce the combination of such components outside of the United States in a manner that infringes claims of the '566 Patent including claim 49.

149. Avigilon commonly supplies such components, preloaded and configured with its Control Center software. Avigilon also specifically states that its “Network Video Recorders (NVRs) have Avigilon Control Center (ACC) software preloaded and configured for exceptional performance and reliability, making them easy to integrate into Avigilon surveillance systems.”¹ Furthermore, “ACC Professional high-performance remote monitoring workstations are designed to complement HD NVRs in an Avigilon HD surveillance system. Pre-loaded with

¹ Avigilon Video Surveillance Record and View Solutions Quick Selection Guide, p. 3, available at <http://4a54f0271b66873b1ef4-ddc094ae70b29d259d46aa8a44a90623.r7.cf2.rackcdn.com/assets/Uploads/avigilon-record-and-view-quick-selection-guide-en-rev3.pdf>.

ACC Client software, the remote monitoring workstation is easily installed to add an additional monitoring station to an existing system.”²

150. Avigilon commonly supplies such components, preloaded and configured with its Control Center software, from its manufacturing facility in Plano, Texas. For example, according to a February 2017 Avigilon press release, Avigilon’s North American “facilities provide direct access to the global markets we sell to.”³ Moreover, Avigilon admits that “with manufacturing facilities in Plano, USA and Richmond, Canada, as well as regional offices around the world, Avigilon solutions are sold and supported throughout the global security market.”⁴

151. As a reasonable inference based on the foregoing allegations, Avigilon has sold its Control Center software loaded on NVRs, workstations, or appliances from its Texas locations to customers in the United States and outside the United States.

152. Avigilon instructs its customers to connect Avigilon’s NVRs, workstations, appliances, and/or cameras to a network.

² Avigilon Video Surveillance Record and View Solutions Quick Selection Guide, p. 6, available at <http://4a54f0271b66873b1ef4-ddc094ae70b29d259d46aa8a44a90623.r7.cf2.rackcdn.com/assets/Uploads/avigilon-record-and-view-quick-selection-guide-en-rev3.pdf>.

³ <http://avigilon.com/news/security/avigilon-dna-a-success-story-made-in-north-america/>

⁴ Avigilon Video Surveillance Solutions Product Brochure, p. 3, available at <http://4a54f0271b66873b1ef4-ddc094ae70b29d259d46aa8a44a90623.r7.cf2.rackcdn.com/assets/Uploads/avigilon-video-surveillance-solutions-product-brochure-en-rev4.pdf>

153. Avigilon instructs its customers to combine Avigilon's NVRs, workstations, appliances, and/or cameras.

154. As a reasonable inference based on the foregoing allegations, at least one of Avigilon's customers connects Avigilon's NVRs, workstations, appliances, and/or cameras to a network outside the United States.

155. As a reasonable inference based on the foregoing allegations, at least one of Avigilon's customers combines an Avigilon NVR—loaded with Control Center software—with an Avigilon workstation—loaded with Control Center software—and Avigilon cameras outside the United States.

156. Avigilon commonly supplies or causes to be supplied in or from the United States components especially made and/or adapted for use in the inventions to which claims of the '566 Patent are directed. As just one example, Avigilon commonly supplies or causes to be supplied in or from the United States components especially made and/or adapted for use in the invention to which claim 49 of the '566 patent is directed.

157. In circumstances where such a component is uncombined in whole or in part, Avigilon supplies the component—including but not limited to software, NVRs, workstations, appliances, encoders, and cameras—knowing that such component is especially made and/or adapted for use in the inventions to which claims of the '566 Patent are directed including the invention of claim 49.

158. Avigilon's actions in this regard demonstrate that it intends that such component will be combined outside of the United States in a manner that infringes claims of the '566 Patent including claim 49. Avigilon commonly supplies such components, preloaded and configured with Avigilon Control Center software, from its manufacturing facility in Plano, Texas.

159. As described above, Avigilon's Control Center video management software and the Avigilon hardware with which it is used—including but not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras—have no substantial non-infringing use. In order to use Avigilon's software and hardware systems to provide any intended use, the claims of the '566 Patent are practiced.

160. The reasonable inference drawn from the facts set forth above in Paragraphs 63-76 is that Avigilon's Control Center software, the Avigilon Blue Cloud Service software, and the Avigilon hardware with which it is used—including but not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras—are a material part of the system claimed in the '566 Patent and that it is not a staple item of commerce. Avigilon's Control Center software and the Avigilon hardware with which it is used have no use without infringing the '566 Patent. Plaintiff asserts that this reasonable inference is true.

161. Another reasonable inference from the facts set forth above is that Avigilon knowingly and actively induced—and continues to induce—its customers

to install its Control Center software on a computer with connected servers and cameras. Avigilon specifically manufactures, markets, and sells hardware designed to be used in conjunction with its video surveillance software including the Control Center software and the Avigilon Blue Cloud Service software. Such hardware includes but is not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras. By providing these software and hardware components and instructing customers to combine the components in the ways described above, Avigilon knowingly and actively requires its customers to infringe the '566 Patent. Plaintiff asserts that this reasonable inference is true.

162. Avigilon and its customers directly infringe the '566 Patent by their use of the Avigilon Control Center software and the associated Avigilon hardware.

163. Based on the facts alleged above, it is a reasonable inference that Avigilon knew that its software was especially made or adapted for use to infringe the '566 Patent when it sells its Control Center software.

164. Plaintiff has suffered damages as a result of the infringing activities of Avigilon, and will continue to suffer such damages as long as those infringing activities continue.

165. Avigilon had knowledge of the '566 Patent at least as early as the filing of the original Complaint in this Action. If Avigilon asserts that it had no knowledge

of the '566 Patent prior to the filing of the original Complaint in this Action, Avigilon was willfully blind to a competitor's patent rights.

166. After knowledge of the '566 Patent, Avigilon continues to infringe the '566 Patent by its sale of Control Center software and the Avigilon hardware with which it is used—including but not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras. After knowledge of the '566 Patent, Avigilon continues to take active steps to market, sell, instruct and support its customers and potential customers of Avigilon's Control Center software and associated Avigilon hardware to infringe the '566 Patent. After knowledge of the '566 Patent, Avigilon continues to advertise on its website its Control Center software used specifically in combination with hardware practicing the '566 Patent.

167. Avigilon causes to be supplied in or from the United States video surveillance software and other video surveillance system components knowing that such components are adapted to be combined outside of the United States in an infringing manner. Avigilon's activities contributorily infringe the '566 Patent.

168. These activities include, but are not limited to, selling Avigilon Control Center software, Avigilon Blue Cloud Service hardware and software, NVRs, workstations, appliances, encoders, and cameras to partners and/or customers outside the United States. By causing infringing components including, but not

limited to, its Control Center software, to be supplied from the United States, Avigilon is infringing claims of the '566 Patent under 35 U.S.C. § 271(f)(2).

169. Avigilon causes to be supplied in or from the United States, video surveillance software and other video surveillance system components in such a manner as to actively induce the combination of such video surveillance system components outside of the United States in an infringing manner. Avigilon's activities induce infringement the '566 Patent.

170. These activities include, but are not limited to, selling Avigilon Control Center software, Avigilon Blue Cloud Service hardware and software, NVRs, workstations, appliances, encoders, and cameras to partners and/or customers outside of the United States, and requiring, instructing and supporting their use to infringe the '566 Patent. For example, Avigilon Control Center software is designed such that the only use of the software is to infringe the '566 Patent. Avigilon is infringing claims of the '566 Patent under 35 U.S.C. § 271(f)(1).

171. It is reasonable to infer based on the facts set forth above in Paragraphs 18-40 and 63-103, that Avigilon's conduct has been willful, wanton and deliberate. It is also reasonable to infer that Avigilon's actions have been objectively reckless based on the facts set forth in Paragraphs 18-40 and 63-103 above. The actions of Avigilon with regard to infringement of the '566 Patent are willful such that JDS is entitled to treble damages under 35 U.S.C. § 284.

172. After knowledge of the '566 Patent, Avigilon continues to infringe the '566 Patent.

173. Avigilon is a substantially larger company than JDS. It would, therefore, be reasonable to infer that Avigilon believed that it could infringe the '566 Patent with impunity based on its size advantage over JDS.

174. Plaintiff has suffered damages as a result of the infringing activities of Avigilon, and will continue to suffer damages as long as those infringing activities continue.

175. Plaintiff has no adequate remedy at law. Unless enjoined by this Court, Avigilon will continue such willful acts of infringement, causing Plaintiff to incur substantial and irreparable damages.

**X. COUNT VI – INFRINGEMENT OF USPN 8,185,964 UNDER
35 U.S.C. § 271(f)**

176. Plaintiff repeats and re-allege the allegations contained in Paragraphs 1-175 above as if fully set forth herein.

177. Plaintiff specifically incorporates here each of its allegations in connection with Count IV regarding indirect infringement of the '964 Patent, which are set forth in Paragraphs 104-144 above.

178. Avigilon commonly supplies or causes to be supplied in or from the United States all or a substantial portion of the components recited in claims of the '964 Patent. As one example, Avigilon commonly supplies or causes to be supplied in or from the United States all or a substantial portion of the components used to practice the method recited in claim 1 of the '964 Patent.

179. In circumstances where such components are uncombined in whole or in part, Avigilon supplies these components—including but not limited to software, network video recorders (NVRs), workstations, appliances, encoders, and cameras—in such manner as to actively induce the combination of such components outside of the United States in a manner that infringes claims of the '964 Patent including claim 1.

180. Avigilon commonly supplies such components, preloaded and configured with its Control Center software. Avigilon specifically states that its “Network Video Recorders (NVRs) have Avigilon Control Center (ACC) software preloaded and configured for exceptional performance and reliability, making them easy to integrate into Avigilon surveillance systems.”⁵ Furthermore, “ACC Professional high-performance remote monitoring workstations are designed to complement HD NVRs in an Avigilon HD surveillance system. Pre-loaded with

⁵ Avigilon Video Surveillance Record and View Solutions Quick Selection Guide, p. 3, available at <http://4a54f0271b66873b1ef4-ddc094ae70b29d259d46aa8a44a90623.r7.cf2.rackcdn.com/assets/Uploads/avigilon-record-and-view-quick-selection-guide-en-rev3.pdf>.

ACC Client software, the remote monitoring workstation is easily installed to add an additional monitoring station to an existing system.”⁶

181. Avigilon commonly supplies such components, preloaded and configured with its Control Center software, from its manufacturing facility in Plano, Texas. For example, according to a February 2017 Avigilon press release, Avigilon’s North American “facilities provide direct access to the global markets we sell to.”⁷ Moreover, Avigilon admits that “with manufacturing facilities in Plano, USA and Richmond, Canada, as well as regional offices around the world, Avigilon solutions are sold and supported throughout the global security market.”⁸

182. As a reasonable inference based on the foregoing allegations, Avigilon has sold its Control Center software loaded on NVRs, workstations, or appliances from its Texas locations to customers in the United States and outside the United States.

183. Avigilon instructs its customers to connect Avigilon’s NVRs, workstations, appliances, and/or cameras to a network.

⁶ Avigilon Video Surveillance Record and View Solutions Quick Selection Guide, p. 6, available at <http://4a54f0271b66873b1ef4-ddc094ae70b29d259d46aa8a44a90623.r7.cf2.rackcdn.com/assets/Uploads/avigilon-record-and-view-quick-selection-guide-en-rev3.pdf>.

⁷ <http://avigilon.com/news/security/avigilon-dna-a-success-story-made-in-north-america/>

⁸ Avigilon Video Surveillance Solutions Product Brochure, p. 3, available at <http://4a54f0271b66873b1ef4-ddc094ae70b29d259d46aa8a44a90623.r7.cf2.rackcdn.com/assets/Uploads/avigilon-video-surveillance-solutions-product-brochure-en-rev4.pdf>

184. Avigilon instructs its customers to combine Avigilon's NVRs, workstations, appliances, and/or cameras.

185. As a reasonable inference based on the foregoing allegations, at least one of Avigilon's customers connects Avigilon's NVRs, workstations, appliances, and/or cameras to a network outside the United States.

186. As a reasonable inference based on the foregoing allegations, at least one of Avigilon's customers combines an Avigilon NVR—loaded with Control Center software—with an Avigilon workstation—loaded with Control Center software—and Avigilon cameras outside the United States.

187. Avigilon commonly supplies or causes to be supplied in or from the United States components especially made and/or adapted for use in the inventions to which claims of the '964 Patent are directed. As just one example, Avigilon commonly supplies or causes to be supplied in or from the United States components especially made and/or adapted for use in the invention to which claim 1 of the '964 patent is directed.

188. In circumstances where such a component is uncombined in whole or in part, Avigilon supplies the component—including but not limited to software, NVRs, workstations, appliances, encoders, and cameras—knowing that such component is especially made and/or adapted for use in the inventions to which claims of the '964 Patent are directed including the invention of claim 1.

189. Avigilon's actions in this regard demonstrate that it intends that such component will be combined outside of the United States in a manner that infringes claims of the '964 Patent including claim 1. Avigilon commonly supplies such components, preloaded and configured with Avigilon Control Center software, from its manufacturing facility in Plano, Texas.

190. As described above, Avigilon's Control Center video management software and the Avigilon hardware with which it is used—including but not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras—have no substantial non-infringing use. In order to use Avigilon's software and hardware systems to provide any intended use, the claims of the '964 Patent are practiced.

191. The reasonable inference drawn from the facts set forth above in Paragraphs 104-117 is that Avigilon's Control Center software, the Avigilon Blue Cloud Service software, and the Avigilon hardware with which it is used—including but not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras—are a material part of the method claimed in the '964 Patent and that they are not a staple item of commerce. Avigilon's Control Center software and the Avigilon hardware with which it is used have no use without infringing the '964 Patent. Plaintiff asserts that this reasonable inference is true.

192. Another reasonable inference from the facts set forth above is that Avigilon knowingly and actively induced—and continues to induce—its customers

to install its Control Center software on a computer with connected servers and cameras. Avigilon specifically manufactures, markets, and sells hardware designed to be used in conjunction with its video surveillance software including the Control Center software and the Avigilon Blue Cloud Service software. Such hardware includes but is not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras. By providing these software and hardware components and instructing customers to combine the components in the ways described above, Avigilon knowingly and actively requires its customers to infringe the '964 Patent. Plaintiff asserts that this reasonable inference is true.

193. Avigilon and its customers directly infringe the '964 Patent by their use of the Avigilon Control Center software and the associated Avigilon hardware.

194. Based on the facts alleged above, it is a reasonable inference that Avigilon knew that its software was especially made or adapted for use to infringe the '964 Patent when it sells its Control Center software.

195. Plaintiff has suffered damages as a result of the infringing activities of Avigilon, and will continue to suffer such damages as long as those infringing activities continue.

196. Avigilon had knowledge of the '964 Patent at least as early as the filing of the original Complaint in this Action. If Avigilon asserts that it had no knowledge

of the '964 Patent prior to the filing of the original Complaint in this Action, Avigilon was willfully blind to a competitor's patent rights.

197. After knowledge of the '964 Patent, Avigilon continues to infringe the '964 Patent by its sale of Control Center software, Avigilon Blue Cloud Service software, and the Avigilon hardware with which it is used—including but not limited to Avigilon's NVRs, workstations, appliances, encoders, and cameras. After knowledge of the '964 Patent, Avigilon continues to take active steps to market, sell, instruct and support its customers and potential customers of Avigilon's Control Center software and associated Avigilon hardware to infringe the '964 Patent. After knowledge of the '964 Patent, Avigilon continues to advertise on its website its Control Center software used specifically in combination with hardware practicing the '964 Patent.

198. Avigilon causes to be supplied in or from the United States, video surveillance software and other video surveillance system components knowing that such components are adapted to be combined outside of the United States in an infringing manner. Avigilon's activities contributorily infringe the '964 Patent.

199. These activities include selling the Avigilon Control Center software, Avigilon Blue Cloud Service hardware and software, NVRs, workstations, appliances, encoders, and cameras to partners and/or customers outside the United States. By causing infringing components including, but not limited to, its Control

Center software, to be supplied from the United States, Avigilon is infringing claims of the '964 Patent under 35 U.S.C. § 271(f)(2).

200. Avigilon causes to be supplied in or from the United States video surveillance software and other video surveillance system components in such a such a manner as to actively induce the combination of such video surveillance system components outside of the United States in an infringing manner. Avigilon's activities induce infringement the '964 Patent.

201. These activities include selling the Avigilon Control Center software, Avigilon Blue Cloud Service platform, NVRs, workstations, appliances, encoders, and cameras to partners and/or customers, outside of the United States, and requiring, instructing and supporting their use to infringe the '964 Patent. For example, Avigilon Control Center software is designed such that the only use of the software is to infringe the '964 Patent. Avigilon is infringing claims of the '964 Patent under 35 U.S.C. § 271(f)(1).

202. It is reasonable to infer based on the facts set forth above in Paragraphs 18-22, 44-59, and 104-144, that Avigilon's conduct has been willful, wanton and deliberate. It is also reasonable to infer that Avigilon's actions have been objectively reckless based on the facts set forth in Paragraphs 18-22, 44-59, and 104-144 above. The actions of Avigilon with regard to infringement of the '964 Patent are willful such that JDS is entitled to treble damages under 35 U.S.C. § 284.

203. After knowledge of the '964 Patent, Avigilon continues to infringe the '964 Patent.

204. Avigilon is a substantially larger company than JDS. It would, therefore, be reasonable to infer that Avigilon believed that it could infringe the '964 Patent with impunity based on its size advantage over JDS.

205. Plaintiff has suffered damages as a result of the infringing activities of Avigilon, and will continue to suffer damages as long as those infringing activities continue.

206. Plaintiff has no adequate remedy at law. Unless enjoined by this Court, Avigilon will continue such willful acts of infringement, causing Plaintiff to incur substantial and irreparable damages.

XI. DEMAND FOR RELIEF

In accordance with the foregoing, Plaintiff respectfully demands that this Court enter judgment:

A. Declaring that Avigilon has infringed the claims of the '566 Patent and that such infringement has been and continues to be willful;

B. Declaring that Avigilon has infringed the claims of the '964 Patent and that such infringement has been and continues to be willful;

C. Preliminarily and permanently enjoining and restraining Avigilon, its officers, directors, employees, agents, servants, successors and assigns, and any and all persons acting in privity or in concert with Avigilon, from further infringement of the '566 and '964 Patents;

D. Awarding Plaintiff its damages, together with prejudgment interest and costs, and increasing those damages to three times the amount found or assessed as provided by 35 U.S.C. § 284;

E. Declaring this an exceptional case within the meaning of 35 U.S.C. § 285, and awarding Plaintiff its reasonable attorney's fees and costs and disbursements in this action; and

F. Granting to Plaintiff such other and further relief as this Court deems reasonable.

XII. DEMAND FOR JURY TRIAL

Plaintiff respectfully demands a trial by jury of any and all issues so triable.

Respectfully submitted,

BROOKS KUSHMAN P.C.

Dated: July XX, 2018

By: /s/

Mark A. Cantor (P32661)

Marc Lorelli (P63156)

Jonathan Nikkila (P75666)

Todd Dishman (P77652)

1000 Town Center, Twenty-Second Floor

Southfield, Michigan 48075

Telephone: (248) 358-4400

Facsimile: (248) 358-3351

Email: mcantor@brookskushman.com

mlorelli@brookskushman.com

jnikkila@brookskushman.com

tdishman@brookskushman.com

Attorneys for Plaintiff